APPROACHES TO SUPPORT FAMILIES' ENGAGEMENT WITH CYBER SECURITY FOR HOME IOT DEVICES

A THESIS SUBMITTED TO
The University of Kent
IN THE SUBJECT OF COMPUTER SCIENCE
FOR THE DEGREE
OF PHD.

By
Sarah Turner
April 2023

Abstract

This thesis records research carried out to explore how families in the UK understand and manage the cyber security of Internet of Things (IoT) devices they use in their homes (home IoT devices), using a variety of research methods. It initially engaged parents and children to understand what they think when discussing the cyber security threats and risks that home IoT devices pose and what they do to mitigate the issues they are concerned about. The findings of those discussions then led to a review of the advice individuals may encounter when searching for answers about cyber security online. These discussions also precipitated a period of autoethnography, a reflexive piece of research that allowed the researcher to consider the extent to which cyber security actually occurs in daily life in a family context. These initial pieces of research provided a picture of families — both adults and children — keen to use home IoT devices but not really understanding either how they work or how to learn about and manage the threats and risks that the devices pose in the home. The thesis uses the Transtheoretical Method of Behaviour Change (TTM) as a theoretical base for reflecting upon the place of participant families on the cycle of adoption of cyber security for their home IoT devices. Using this model, it was possible to understand that participant families were, on the whole, at the very first stage of the cycle — precontemplation, and that the information that they might rely upon is insufficiently robust to support knowledge gathering and raise awareness. Hurdles at home around finding the opportunity to discuss cyber security, or even having the appropriate vocabulary, could also hinder efforts to understand the topic better. To move further along the TTM cycle, training and education would be required to increase their levels of awareness.

To work with families to understand what interventions families may need to increase their awareness of cyber security measures for home IoT devices, a piece of user-centred design work was undertaken to create a serious game. Serious games have been successfully used in organisational and educational settings to teach and explore cyber security concepts before, but not with families at home. The game represented an opportunity to provide participants' families with information on cyber security as it pertains to home IoT devices. This allowed participant families to receive information and possibly move around the TTM cycle at least to the step beyond precontemplation: contemplation. This was evidenced in discussions during and after gameplay about wanting to make changes to their home cyber security setup. In some cases, it was hoped that participants could move further around the cycle to take action, having been motivated by the knowledge provided in the game.

When playing the game, families were given the opportunity to learn about the type of cyber security concerns that could arise in relation to home IoT devices and asked if they would make any modifications to the cyber security measures they use at home in the week following the game. Significantly, more of the gameplay participants did take action to change their cyber security setup in the week following gameplay than a control group that had not had the opportunity to play the game. Almost all participant families discussed their cyber security setup at home during the period of gameplay, and several also reported continuing this discussion in the week following the game, evidencing that the game raised sufficient awareness within the participant families to be able to have conversations about the topic. This suggested that the game could stand as a tool for awareness raising by itself; however, the process of gameplay exposed several other areas where interventions outside the family unit should be made.

This thesis makes several novel contributions, both in terms of the methods used and the findings arising from them. It provides evidence on the level of knowledge within families in the UK about the home IoT devices that they use, how they use them, and their level of comfort with their cyber security setup. Through discussions with participant families and analysis of survey results, the reliance on the Internet for the gathering of knowledge in relation to home IoT device cyber security questions or concerns is made clear. By subsequently analysing the appropriateness of available cyber security information for Internet users, the thesis highlights the lack of visibility of sources to provide targeted and robust guidance. There was also a complete lack of awareness from all participants as to the official governmental agency in the UK from which to gain cyber security guidance. Engaging with participant families over the period of the research consistently highlighted the ease with which cyber security and online safety are conflated in training and education provided at school and thus brought into discussions at home. It is also the case that there is an overwhelmingly strong focus on financial ends rather than identity-driven ones: the value of devices (in terms of replacement) and financial loss are what families worry about, not data loss or possible physical threats emanating from home IoT device use.

The use of an autoethnographic diary study provided a means to use reflexive research to explore issues around lack of awareness, conflation of online safety and cyber security, and the difficulty of finding available information online. It further uncovered difficulties that families may have in describing cyber security issues and requirements, simply because the terminology is too complicated, the actions are too complex (or boring), or the end result does not obviously make a difference. Finally, the use of user-centred design with participant families to develop a serious board game, to build awareness, as evidenced in discussion about home IoT device cyber security measures is novel. Analysis of the participant families' interaction with and actions arising from gameplay show that given training and education, families will use this knowledge to facilitate discussion on the subject, but they may need guidance to ensure that they are discussing topics appropriately. It also showed that, being motivated to take action as a result of gaining knowledge from gameplay, families may attempt to make changes to their cyber security setup for home IoT devices, with varying levels of success and appropriate use. Single-action measures (such as setting up a guest network) are the most popular, although perhaps not the most effective, in terms of managing common cyber security problems. Repetitive actions (such as turning devices off when not in use) seem to quickly fall out of favour, despite being relatively effective and inexpensive, financially at least, to implement. All of these aspects allow for a range of recommendations for improvements to help families have safe home IoT devices.

Acknowledgements

A PhD is a long time in the making, but in reflecting over the course of this work, what has struck me is less the time, and more that, although my name may be on the cover, it has taken a village — or maybe, more accurately, a small city — of truly excellent people to get it to this point.

First and foremost, I must give enormous thanks to my primary supervisor, Dr. Jason Nurse, and secondary supervisor, Prof. Shujun Li. It has been a privilege to be able to perform this work with your guidance — and I really appreciate the moments where I may have said something quite unexpected ("Why don't I do an autoethnography?" "Hey! Why don't I build a board game?!") and you...let me run with it. It has been a lot — a lot — of fun. What shall we do the next one on?

I also want to extend massive thanks to Nandita and Matthew for being the trusty "researchers" and "second coders" referenced in parts of this text. Rich, Sarah and Laura at NCSC — thank you for your support in getting this done. Similarly — thank you to Dr. Virginia Franquiera, Dr. Simon Parkin and Prof. Lynne Coventry for being my internal and external examiners, and suggesting some really very smart and sensible suggestions for improvement. Also: all my participants — you all made this feel like the opposite of work.

Going back right to the very start: without the support and belief of Leonie, who let me go phenomenally big on the dissertation element of my MPA, I would never have realised that research was a thing that I could do in a way that others might want to read, use and build upon. All the research that has followed to date is because she allowed me the space (and a little bit of money) to try in the first place: thank you.

Doing a PhD can be extremely isolating — especially when doing it at home, alone, in an office at the end of your garden, during a pandemic. I have been so privileged to be able to, concurrently, work on other pieces of research, helping both my research skills and my sanity. Huge thank yous to: the Kent/RUSI ransomware group (Jamie, Gareth, Pia and James); the Digital Futures Commission team (in particular Kruakae, Sonia, Ayça and Louise) and the CHAI team (especially Mina, Laura and George). I must also extend huge gratitude to Eleanor, Jessica, Douglas, Nerys, Claire and everyone else who has been part of the Monday morning writing group over the last 3 years; also the BfN board, staff and volunteers, who have allowed me to do helpful things that didn't require writing papers about them.

My friends and family — thank you for: Hannah: all the friendship homework — I wouldn't read Twitter without you (and special thank you to Miriam for being an excellent cat). SKB and Kim: being there to share my confusion as the world burns. July: feeding me arequipe as a medicinal cure and being my digital tech policy partner-in-crime. Ben: I'd have been stumped without your 3D printers and your skill — thank you! Mum and Dad: you don't really know what on earth I've been doing, but thank you for not giving me a massively hard time about it. Alicia: without you, we would not be fed, the girls would never be picked up from school, and I would have done a tiny fraction of all of this. You are the person who has, truly, facilitated all of this with only three emergency hospitalisations and no mental breakdowns. A massive win all around.

Andy: you were mad I started this, but proud by the end — phew. Thank you for being there for *Spaced* quotes, in-jokes, coffee, tea (*twelve's my limit*), doing all the hoovering and all the nonsense that was 2020–today.

Bea and Rosie: I know you won't want to hear it, but you are the reason this thesis looks at the relationships between parents and children. As such, I apologise for spending three years figuring out how to ruin the Internet for you.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

This chapter will introduce the topic of the thesis and give background as to the motivation behind it. As Internet of Things (IoT) devices become increasingly common in the home, the need for considerations about the cyber security of such devices becomes more pressing. This thesis will consider the sociotechnical implications of this for a particular group: UK families with school-aged children. What level of awareness of the cyber security needs of home IoT devices do families have? What information is available to them and what problems do they face when trying to manage the cyber security of home IoT devices? And what support may they need to promote positive cyber security actions for these devices?

This chapter continues as follows. Section 1.1 provides an overview of various background aspects related to the research presented in the thesis. Section 1.2 provides details on the research aims, questions and contributions, and Section 1.3 provides an overview of the structure of the thesis.

1.1 Background

1.1.1 The introduction of IoT into the home

The concept of computers in the home is not new, with the first home computers introduced more than 40 years ago (Computer History Museum 2023). Computer processing capabilities have grown massively in this time, and the adoption of the Internet has firmly established digital technologies in the home, both in devices that resemble computers and, increasingly, in other devices. There has been significant research into how home computer users approach and manage the security of their computer use (for example, Howe et al. (2012); Furnell, Bryant and Phippen (2007); Wash (2010); Thompson, McGill and Wang (2017)), and as people spend more time using social media and sharing personal information on the Internet, research has looked at how people also consider their privacy in relation to digital technologies.

Figures from the market data company Statista suggest that the consumer segment consists 60% of the 9.76 billion IoT devices used in 2020; a figure that was estimated to increase to 17.08 billion by 2024 (Vailshery 2022). A 2022 report on the ownership of smart home products in the UK found that 77% of the respondents owned at least one such device, with 88% of the people surveyed having some level of knowledge around smart homes — and 37% claiming to have high or very high levels of knowledge (techUK and GfK 2022). Although the picture of ownership is complex, with only smart TVs, smart home assistants, and fitness devices reported in this survey as having ownership levels higher than 20% of the respondent population, the increase of such devices in communal areas of the home cannot be denied. This means that all members of a household, whether adults or children,[1] comfortable with technology or not, may be expected to live around devices connected to the Internet.

The user's feelings about IoT devices and privacy, which for the purposes of this work is considered a subset of a wider field of cyber security, has been considered in quite some depth in recent research. IoT devices often look and feel significantly different from computers, and as such users may not understand how to mitigate cyber security threats[2] and subsequent risks[3] or even that such devices have the

[1] Throughout this thesis, "child" will be used to consider any individual 18 or under living in the same home as their parents, legal guardians or caregivers. We will use the term "parents" to broadly refer to parents, legal guardians, or caregivers.

[2] The US government's National Institute of Standards and Technology (NIST) defines a cyber security threat to an individual as: "Any circumstance or event with the potential to adversely impact...individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service." (National Institute of Standards and Technology ndb)

[3] NIST defines a cyber security risk to an individual as: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." (National Institute of Standards and Technology nda)

potential to pose threats and risks. Furthermore, the very concept of a user may be misleading in the context of devices that are designed to be used in communal areas, such as homes. This work will focus on families — at least one adult parent or legal guardian, and one child of school age or younger[4] — there remain numerous unresolved questions concerning how individuals of varying ages, with varying degrees of access and control over devices, and comprehension interact with and utilise these gadgets.

The IoT is a vague concept with no specific definition or boundaries. Typical definitions are usually of the form "physical devices... that are now connected to the Internet, all collecting and sharing data" (Ranger 2020), with no clear distinction of whether, for example, a smartphone or any other device with a SIM card in, would be included in the definition. For the purposes of this work, and in line with the focus of research in the United Kingdom (UK), the term "home IoT devices" will be used to refer to such devices explicitly defined in the Code of Practise for Consumer IoT Security (Code) defined by the UK Government Department of Digital, Culture, Media and Sport (DCMS) (Department for Digital, Culture, Media and Sport 2018).[5] Although a non-exhaustive list in the Code, it will be considered exhaustive for the purposes of this work to ensure a definitive list of devices. This list is:

- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Smart cameras, TVs and speakers
- Wearable health trackers
- Connected home automation and alarm systems
- Connected appliances (e.g., washing machines, fridges)
- Smart home assistants

[4] For more explanation on how this has been defined and considered in this work, see Chapter 3.6.

[5] As of February 2023, the remit for digital governance in the UK government has been reassigned to the Department for Science, Innovation and Technology from DCMS. DCMS will be mentioned primarily in this thesis, as the owner and actor behind the documents and policy mentioned.

Although not all devices in this list are devices used in home settings by multiple users, this list covers several devices that may be present in the family context. Therefore, the use of the phrase “home IoT devices” will be made reference to this list.[6] Even within this list, it should be noted that two types of device predominate in the homes of UK residents at this time: smart TVs — including devices that plug into a television to enable streaming of content, such as Google Chromecast and Amazon Fire TV Stick — and smart home assistants, such as Google Home and Amazon Echo (techUK and GfK 2022). As is also mentioned in the Code, consideration of such devices necessarily includes the “associated services” that form part of the IoT ecosystem: in particular, they are described as “mobile applications, cloud computing/storage, and third party Application Programming Interfaces”. It is relatively clear that many home IoT devices will require their primary user (or users) to interact with it through a mobile application (app), and if data processing is done remotely, it will be done using cloud computing, with data stored “in the cloud”. However, in many cases, given the relative novelty of home IoT devices and the lack of interoperability between devices made by different manufacturers or different generations of devices made by one manufacturer, users may need to turn to third-party software or applications to get devices from different manufacturers to interact with each other.[7]

The privacy and security of all people living within a home are of key importance when considering home IoT devices. Keeping data that are intended to be private out of the public domain is fundamental, but the security issues that arise from the adoption of home IoT devices extend beyond this. The relative novelty and heterogeneity of such devices, coupled with their global production, also mean that, until recently, they have evaded meaningful explicit regulation or legislation to mandate minimum security requirements. In the UK, the jurisdiction in which this thesis will focus its research on, an act passed in December 2022 (although not implemented at the time of writing this thesis), the Product Security and Telecommunications Infrastructure Act (2022) (PSTI Act) requires that home IoT devices are not sold with default passwords, have a defined period of support and a contact for vulnerability disclosure. Until such law is implemented, it will

[6] It should be noted that the remit of the newly passed Product Security and Telecommunications Infrastructure Act (2022) extends beyond the Code, to include smartphones and computers, signaling a move to consolidate obligations for all consumer digital technologies.

[7] Such as IFTTT (“If This, Then That”) — `https://ifttt.com/`.

remain unclear not only whether such minimum obligations will be meaningful in changing manufacturer behaviour, but also how well such a law can be enforced.[8]

IoT devices are often brought to the home by one keen individual, who maintains them after installation (Geeng and Roesner 2019; Strengers et al. 2019), or possibly simply brought to the house because there was no option to have a “dumb” device (e.g., smart TVs constitute the majority of TVs available for purchase) at the place of purchase, or because a landlord has required it. This means that there is the potential for a level of required acquiescence from all household members when an IoT device is brought into the home. Relationships between parents and children are typically unequal in terms of control, resources, and knowledge, despite there being an increasing democratisation between parents and children in decision making about family life (Blum-Ross and Livingstone 2020; Gadlin 1978). Parents are more likely to have the financial ability to bring devices into the home and determine the way the device is used within it. Although older children may have some resources to buy smart home assistants or connected toys, for example, research has shown that the types of devices that parents may buy will be for much wider applications, including, for example, protection of the home, which could well be to the detriment of the privacy of children (or others) in the household (Ur, Jung and Schechter 2014; Ghosh et al. 2018).

This thesis will provide further research needed to understand the most appropriate way to help families manage the potential cyber security risks posed by home IoT devices. Conflicts between lack of regulation, general ignorance, and disregard for the security risks that home IoT devices can present are widespread. The power relationships between parents and children show many elements that need to be understood as a whole before being able to assess potentially successful interventions to help families have a more secure smart home.

1.1.2 Home computer security

There has been significant prior research on how people use computers at home. Furnell, Bryant and Phippen (2007) found that 90% of those who use computers at home agree that users are responsible for their security. Despite this, home users have been shown to exhibit risky behaviours, such as disabling automatic

[8] In particular, the Act’s aim at requiring retailers of devices to take care to ensure these standards are met of products they sell may be a very helpful move, if enforced.

updates because they distrust the process (Wash et al. 2014; Forget et al. 2016) and expect security products to protect them in ways that they do not (Christin et al. 2012). According to some research, it is too difficult to implement adequate security measures and there is too little reward (Mills and Sahi 2019). Even when accurate advice is initially received, users typically form incorrect mental models in relation to how the technology they use works (Wash 2010; Abdi, Ramokapane and Such 2019), or about the type of user or device that is typically targeted in relation to cyber crime (Howe et al. 2012) — this leads to adopting ineffective, albeit perfectly rational, security postures (Herley 2009; Forget et al. 2016).

Targeting the home user for cyber security education has proven difficult. Individuals often find it difficult to find legitimate sources of security knowledge (Howe et al. 2012), and government-driven cyber security awareness schemes often do not provide enough focused actions for individuals to follow (Bada, Sasse and Nurse 2015; Das, Dabbish and Hong 2019). Individuals may only receive security training at work: this training is typically not transferred to the home context (Simonet and Teufel 2019). Even if individuals act to implement cyber security measures at home, they will be overwhelmed with the number of actions that are deemed essential (Redmiles et al. (2020) found 374 pieces of actionable advice when reviewing publicly available documentation).

Often, people rely on the advice of friends or relatives that they esteem highly (Nthala 2019), regardless of whether those asked to help individuals have expert knowledge (Poole et al. 2009). Even if individuals have higher levels of knowledge, it does not always translate into action, and it is questionable as to the level of responsibility that those experts acting privately consider themselves to have after providing the initial suggested solution (Nthala and Flechais 2018). Furthermore, research has shown that men will claim to be knowledgeable, regardless of their level of knowledge: conversely, women will underplay their knowledge (Rode 2010).

Cyber security is increasingly part of school curricula (Kritzinger, Bada and Nurse 2017), however, it is perhaps naïve to assume such lessons will be subsequently shared with the entire family unit; indeed, Blum-Ross and Livingstone (2020) suggests that the relationship between the school and the family unit is such that joined learning between school and home is, on the whole, never considered an option. Understanding the place of cyber security teaching in schools in the UK is complicated by the devolved nature of curriculum setting; however, to minimise complexity in this project, the English Department for Education (DfE) curriculum (Department for Education 2013) has been used, as it is the oldest, and is referenced as a basis for at least some of the more recent devolved nations' curricula.[9]

Having knowledge of computer security does not necessarily translate to smartphones or home IoT devices: Thompson, McGill and Wang (2017) showed that different interfaces and interactions mean that security knowledge is not necessarily transferable between traditional computers and smartphones. Aufner (2020) found that traditional methods of threat modelling for software do not explicitly map onto the IoT, leaving the potential for both developers and individuals to underestimate the risks such devices pose.

1.1.3 Cyber security and the IoT in the home

Research suggests that people see the value of having devices connected to the Internet in the home setting (Singh et al. 2018; Ur, Jung and Schechter 2014). However, the domestic use of such devices extends and alters the potential risks to which users are exposed compared to traditional home computers. Most home IoT devices are explicitly designed to be easy to use and blend into the environment in which they are housed. They are also heterogeneous — there is a wide marketplace, with little standardisation of functionality for individuals to manage security settings.

Significant consideration has already been given to the implications of constant data collection, where IoT devices process data in the cloud (Apthorpe et al. 2018) and the patterns that can be extrapolated from it (Tolmie et al. 2016). The importance of personal data collection for the proper functioning of such devices sees privacy, that is, the safekeeping of personal data, as a vitally important and intertwined subset of the wider cyber security picture when considering home IoT devices. The perceived convenience of such devices shows that people exhibit the privacy paradox when using such devices: despite considering themselves privacy

[9] Within the UK, each of the devolved nations have their own powers to build school curricula. The curricula within Wales, Scotland, and Northern Ireland cover similar ground, focussing on online safety and learning about the role of the Internet within society, in particular.

conscious, in practise, they exhibit risky behaviour, in particular sharing a significant amount of personal information with home IoT devices and further with online services, where the perceived benefit of using such devices is worthwhile (Williams, Nurse and Creese 2016, 2017; Lutz and Newlands 2021). Zheng et al. (2018) found that individuals trust manufacturers to protect their privacy, but do not take steps to verify this. There are therefore both risks that users will provide personal data that they subsequently regret to manufacturers that can be used in ways they are uncomfortable with and also that manufacturers do not protect the data they have in ways that they should to prevent wide-scale data breaches.

However, more difficult than understanding the data that IoT devices collect is how user-level security should be considered. It is not surprising that adherence to recommended cyber security hygiene measures (for example, those found in National Cyber Security Centre, UK (2019); Boeckl et al. (2019)) is poor, when cost and features may be more important than security at the point of purchase Emami-Naeini et al. (2019a), and given that individuals have incorrect mental models in relation to how devices work (Abdi, Ramokapane and Such 2019; Huang, Obada-Obieh and Beznosov 2020). The inability of governmental bodies in the UK to get device producers to adhere to the Code for the safety of such devices, and the subsequent watering-down of these provisions in the PTSI Act, further points to the dual problem that is presented here: there is no mechanism to hold producers to account for producing and selling insecure devices, whilst those buying them do not have the knowledge or interest to ensure that the devices are secure before using them.

The lack of control with such systems poses a risk for users trying things out for novelty's sake, or when they do not fully understand the implications of their actions. Previous research has considered how the complexity, ubiquity, and novelty of IoT requires more user-friendly risk management frameworks at home (Nurse, Atamli and Martin 2016; Chhetri 2019; Prange, von Zezschwitz and Alt 2019). In a household with many users, there will be different levels of technology knowledge and, in the case of a family within the home, different ages, power dynamics of responsibilities, and maturity levels to consider before a truly representative framework can be put in place. At the most fundamental level, a future that foresees smart homes filled with IoT devices performing important tasks in managing the home requires devices that cannot easily be tampered with, broken, or otherwise undermined to inflict damage on the home's inhabitants, whether through accident or malice.

1.1.4 Parents, children, and digital technologies

Historically, children's use of media and, increasingly, digital technologies has been framed in terms of parental mediation. *Restrictive Mediation* by parents sees limitations being placed upon how a child uses the Internet — time, place, length or content restrictions, for example. *Active Mediation* sees parents managing Internet use through discussion and co-use. There is a suggestion from more recent research that a mixture of the two — *Enabling Mediation* (Livingstone et al. 2017) — combines the benefits of both elements: restrictive mediation has been shown in some cases to minimise risky Internet behaviour, while active mediation gives opportunities for learning and resilience building. Restrictive mediation is often used by parents that feel less secure in their understanding of the technologies being used: however, the more widespread the technology, the less realistic it is to use restrictions as a means of control. Livingstone's more recently published research, however, raises dissatisfaction as to the framing of "mediation" as a whole: Blum-Ross and Livingstone (2020) suggest that considering parents policing technology through any form of "mediation" neglects to show any interest in parenting as an activity that engages with children, or considers children as beings with their own agency.

Research into the collaborative use of technology within families often considers young children or teenagers — but not both. Children's use of digital technologies develops and changes as they grow, as do their legal rights to their data.[10] It is fundamental to understand what these changes are and what risks they can pose, to work towards security for the entire household.

[10] The age at which children are given the right to consent to data processing is determined by the relevant jurisdiction(s), and varies between 13 and 16 years old within the European Union, as an example. In the UK, this age is 13.

1.2 Theoretical framing, research aims, questions and contributions

1.2.1 Theoretical framing

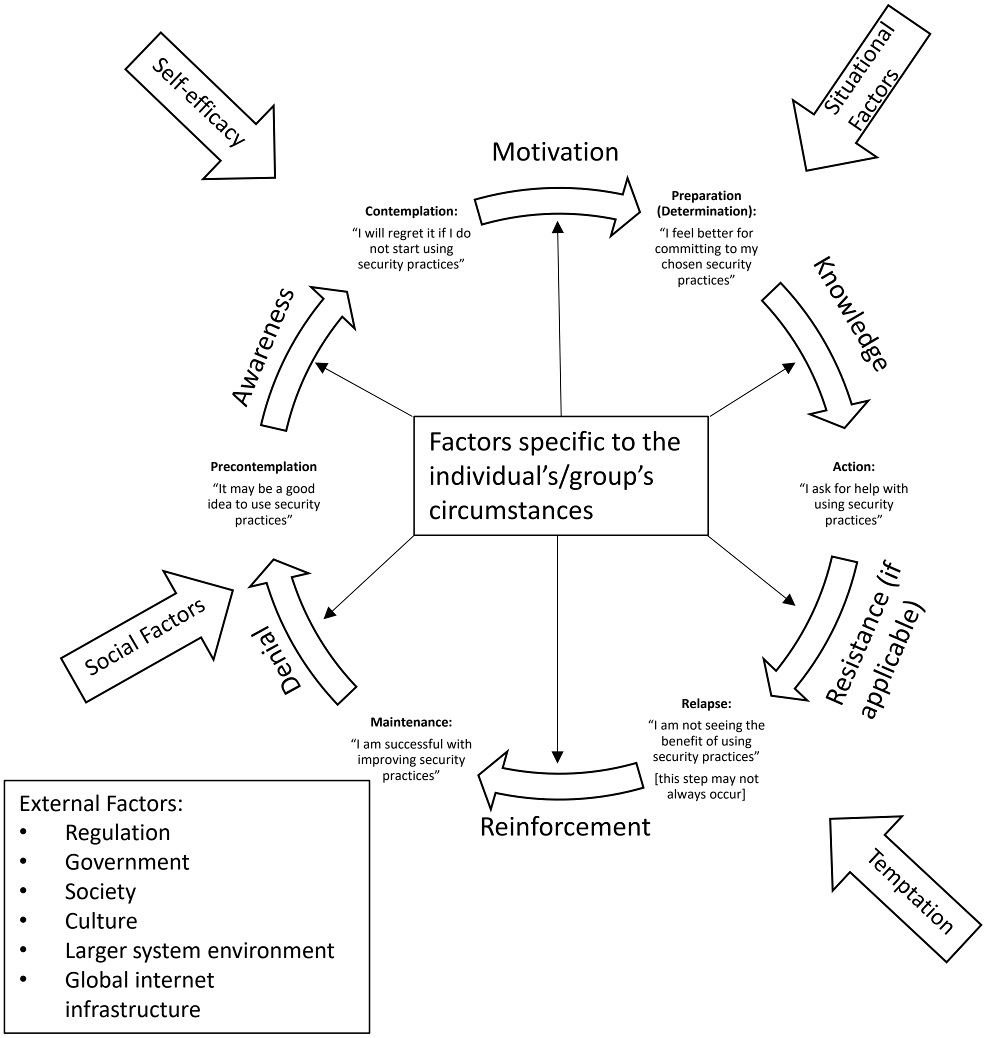
The aims of this thesis should be considered in relation to a particular theory of behaviour change, the Transtheoretical Model of Behaviour Change (TTM), as adapted for cyber security behaviour by Faklaris, Dabbish and Hong (2018). There are several methodologies for behavioural change that have been applied to cyber security (for example, the Theory of Planned Behaviour (Bulgurcu, Cavusoglu and Benbasat 2010) or the Protection Motivation Theory (Ifinedo 2012)). However, TTM considers the journey that a person takes when moving from not knowing about something to maintaining or rejecting the behaviour change through gaining awareness and motivation. This can be done through appropriate education and training, and is how the two concepts overlap: although the concept of awareness, in TTM, is framed solely in terms of moving from "precontemplation" to "contemplation", the role of education and training is vital in that first step in framing contemplative thoughts in an appropriately meaningful and actionable way.

Overall, the research methods chosen in this thesis show a progression based on previous core findings and the need to understand where the user group — families — begin their journey to understand the cyber security of home IoT devices. This is a complex area to unpick carefully, as there are a number of starting places —- and a number of steps to be taken to get to a place where users, in general, will make cyber security changes unprompted. Furthermore, if users do not know that they should be doing anything (in this case, that they should consider employing specific cyber security measures that may be specific to their family's needs and device use), then expecting them to effect any change is futile. This requires a journey of education and training to reach a point of awareness (Amankwa, Loock and Kritzinger 2014). This process is often considered primarily as an organisational one, rather than being applied to individuals in a personal capacity, and thus the definitions typically refer to the need for education, training, and awareness in the workplace. The International Information System Security Certification Consortium defines education as "increasing your knowledge and understanding", training as "improving skills and proficiency with certain tasks" and awareness as "how well acquainted someone is with the education and training needed, or, more importantly, how well acquainted they are with the desired outcome" (Chapple et al. 2021).

As mentioned, the idea of education, training and awareness is considered primarily from an organisational point of view. However, in day-to-day life it can be difficult for an individual to access education or training without some prior awareness of the need to learn. As such, it is vital to consider the state of mind of the users —- in this case, family members — when it comes to implementing cyber security measures on home IoT devices. The one that will be taken into account in this work is TTM, as described by Faklaris, Dabbish and Hong (2018), a framework originally used as a model for initiating and understanding change in public health behaviour. This interpretation of the model is helpful to consider in addition to the above model of education, training, and awareness, as it breaks down the steps an individual may likely take on the journey to maintenance of the desired action (or relapse to old habits). It also recognises the importance of external factors in behaviour change: what are other people doing (social factors), how easy is it to not do the appropriate thing (temptation), and how easy does the society a person is living in make it to effect the right kind of change (regulation, government, society, culture). The model presented in Faklaris, Dabbish and Hong (2018) is reproduced in Figure 1. It is helpful as it starts from the "precontemplation" period (that is to say, before there is awareness), and recognises the need to reframe each step of the journey as a positive construction (e.g. "It may be a good idea to use security practices").

As such, it has been assumed at the start of this work that the first three pieces of research will allow for a sufficiently detailed understanding of where families are on the TTM cycle to build an understanding of the level of information provided as training and educational material in the final piece of research, the game. This is because, as confirmed as the majority position based upon the findings of the interview and survey work, it is assumed that the majority of participant families will need to move from the precontemplation step to contemplation. The game will also provide the measures for allowing participant families to move further around the circle, through "preparation" and "action" stages by giving explanations as to why families may want to change their security practices and how they might go

Figure 1: The Transtheoretical Model of Behaviour Change — reproduced from Faklaris, Dabbish and Hong (2018)



Contemplation:
"I will regret it if I do not start using security practices"

Preparation (Determination):
"I feel better for committing to my chosen security practices"

Precontemplation
"It may be a good idea to use security practices"

Action:
"I ask for help with using security practices"

Maintenance:
"I am successful with improving security practices"

Relapse:
"I am not seeing the benefit of using security practices"
[this step may not always occur]

External Factors:
- Regulation
- Government
- Society
- Culture
- Larger system environment
- Global internet infrastructure

about it. However, crucial steps in relation to positive behaviour change (ending up at "maintenance" as opposed to "relapse") cannot be fully tested in this work, given the time constraints of the project.

1.2.2 Research aim

As such, the first aim of this project is to explore how much awareness the UK-based participant families[11] have about the need to use cyber security measures in relation to the use of home IoT devices. The second aim is to explore how robust the most common technique for solving cyber security problems (searching for information online) is and whether its use is sufficient as a form of awareness in relation to having appropriate cyber security measures in place. The third aim is to explore potential reasons why awareness gaps around the use of appropriate cyber security methods may exist in relation to home IoT devices. Using the information collected while working through the previous three aims, the final aim is to create a test intervention for family participants that uses education and training steps to raise awareness in relation to possible cyber security measures and methods that can be used in relation to home IoT devices.

1.2.3 Research questions

These four aims are reflected in the breakdown of the research questions and the research methods that are used within the thesis. The first three research questions, which encompass the first three pieces of research, explore the level of awareness that participant families have, how successful their main method of managing concerns is, and why other gaps around awareness may exist. The fourth question builds upon the findings of the first three, by understanding if a board game-based intervention can provide a suitable education and training experience to help participant families increase their level of cyber security awareness in relation to home IoT devices.

RQ1: What is the level of awareness exhibited by interviewed and surveyed families

[11] The research within the thesis is limited to families within the UK primarily for reasons of resource. Although many findings will be more broadly applicable than only within the UK, the cultural specificities of family life in the UK may be different than elsewhere. For this reason, the thesis will refer to the UK as the primary geographical location of the research and findings.

in the UK in relation to the cyber security of home IoT devices that they own and use?

RQ2: What knowledge is available online to those who wish to implement cyber security measures for home IoT devices?

RQ3: How can the researcher effectively understand the awareness and motivation to consider the cyber security of home IoT devices shown by families?

RQ4: How can a board game act as an intervention to support participant families to improve awareness in relation to the cyber security of home IoT devices that they own and use?

For more explanation as to how the RQs map to the different parts of the thesis, see Section 1.3.

1.2.4 Original contributions

This research has created a range of original contributions, both in terms of research findings and use of methods.

- Exploration of the level of awareness within families in the UK about the home IoT devices they use, how they collectively use home IoT devices, their level of comfort with their cyber security setup and necessary workarounds to allow use by all family members — *Chapter 4*

- Understanding of the reliance upon the Internet for knowledge gathering in relation to home IoT device cyber security questions or concerns; the absence of credible sources to provide targeted and robust guidance; and the complete lack of awareness of participants as to the official governmental agency in the UK from which to gain cyber security guidance — *Chapter 4, 5*

- Exploration of the ease with which cyber security and online safety are conflated in training and education provided at school and thus brought into discussions in the home — *Chapter 4, 5, 7*

- Setting out the difficulty that families have in describing cyber security issues and requirements, simply because the terminology is too complicated, the actions are too complex (or boring), or the end result does not obviously make a difference — *Chapter 4, 5, 6, 7*

- Recognition of the importance of financial ends rather than identity-driven ones: the value of devices (in terms of replacement) and financial loss are what families worry about, not data loss or possible physical threats emanating from home IoT device use. — *Chapter 4, 7*

- Understanding that given training and education in order to raise awareness, families will use this knowledge to discuss cyber security topics, but they may need guidance to ensure that they are discussing topics appropriately — *Chapter 7*

- Understanding that given training and education, families may attempt to make changes to their cyber security setup for home IoT devices: single-action methods are the most popular, with repetitive actions falling quickly out of favour. — *Chapter 7*

- Analysis of the suitability of the cyber security information available for UK Internet users in relation to the most popularly used home IoT devices by families — *Chapter 5*

- The use of an autoethnographic diary study as a means of embedding reflexive research when considering the ability, capacity, and interests of families in relation to cyber security in the home — *Chapter 5*

- The use of a user-centred design (UCD) process with families to develop a serious board game for families to play, with the aim of improving awareness of threats, risks and mitigation techniques in relation to home IoT devices, and the findings that playing a serious board game with families encourages discussion of cyber security measures and makes participants significantly more likely to introduce changes to their cyber security setup at home in the week after gameplay — *Chapter 6, 7*

- A range of recommendations for relevant stakeholders beyond family units — policymakers, manufacturers (including designers and developers), and academics — as to the ways in which the family use of home IoT devices deviates from what is expected and how best it should be supported through policy, regulatory measures, and improved product design. — *Chapter 8*

1.3 Organisation of Thesis

The rest of the thesis is organised as follows.

1.3.1 Chapter 2: Literature Review

This chapter aims to set out the context of the project and explore the various gaps arising in the research to date. It starts with an overview of the potential harms of home IoT and how users struggle to understand them. It then shifts to consider what research has been done in relation to families and digital technology use: how has this been researched in the past, and how do adults and children perceive home IoT devices, and cyber security now? It finishes with an overview of how research has approached providing solutions to the issues raised.

1.3.2 Chapter 3: An Overview of Methodological Choices

This chapter details the overarching methodological choices and decisions made throughout the thesis. It starts at the highest level, discussing the approach and philosophical views brought to the research; then it goes on to explain the general research methods used. Following that, it explains the process of data collection, preparation, and analysis. It finishes with some brief explanations about the assumptions made in relation to the family unit in the UK, the impact of ethical considerations on the project, and how the project changed as the COVID-19 pandemic progressed.

1.3.3 Chapter 4: Discussing and managing cyber security of home IoT devices

This chapter details the results of the first piece of research undertaken. Following an initial review of the literature, it was decided that the use of an online survey and a set of semi-structured interviews would address the first QR. A survey, in particular, would go some way to answering questions about the types of home IoT devices used, how the decisions were made to use them, and how much knowledge the participants have about security at a broad level across families in the UK. The semi-structured interviews serve as a complement to this, in being able to give more depth and breadth of information around the issues and concerns within a family, and crucially, the opportunity for the entire family to have a say, including children.

1.3.4 Chapter 5: Issues arising when managing the cyber security of home IoT devices

In addition to the survey and interview work, two other pieces of research, carried out at the same time, begin to consider different aspects of the second RQ. An analysis of currently available cyber security awareness information situates the information and perceptions about home IoT device use and security explored in answering the first RQ into the cultural context: what information is objectively available to users, who is producing it, and what does it say — or not say?

The second piece of research, an autoethnographic diary study, looks at how the researcher herself interacts with her family in relation to cyber security discussions and knowledge. This piece of research allows for, possibly, a more nuanced recording of events than might be brought out in an interview (as discussed in Livingstone and Sefton-Green (2016)), over a longer period of time. Importantly, also, it provided a period of reflexivity, which helped to underline the more realistic expectations that families should have when moving into the final piece of research, to understand what interventions might look like.

1.3.5 Chapter 6: The creation of an intervention to promote positive cyber security actions among families: background and setup

This chapter builds upon the previous two and uses the findings from the prior pieces of research to create a serious game for families, to explore if it could serve both as an intervention in and of itself, but also as a tool to understand which elements of cyber security require interventions in different ways. This chapter provides the background to the use of serious games in organisational and educational cyber security learning, the methodology for the research involving the game, and explains the process of creating the initial version of a cyber security board game for families to play.

1.3.6 Chapter 7: The creation of an intervention to promote positive cyber security actions among families: findings

This chapter gives the findings of the serious game research, looking at the outcomes of the user-centred design (UCD) process, and also whether the cyber security learning aspect was carried through into the participants' life in the week following the gameplay session. It goes on to explain the findings; in particular that the UCD element was integral into producing a version of the game with real impact but that there are some consistent aspects of cyber security that were too difficult for families to implement.

1.3.7 Chapter 8: Conclusions

This chapter ties together the other chapters, detailing the answers to the RQs, and presents recommendations that follow on from the findings of the thesis, whilst being mindful of the limitations of this work, and how it could be taken forward in the future.

1.3.8 Publications

At the time of the completion of the thesis, the following works have been published and presented in relation to the overall project.

Initial abstract relating to the project

Sarah Turner. *Approaches and Technologies to Support Home Users' Engagement with Cyber Security.*
Proceedings of the 33rd International BCS Human Computer Interaction Conference (BCS HCI 2020) `https://doi.org/10.14236/ewic/HCI20DC.14`

This paper outlined the initial thoughts relating to the direction of the doctoral project before the undertaking of any research.

Publications relating to Chapter 4

Sarah Turner, Nandita Pattnaik, Jason R.C. Nurse, and Shujun Li. 2022. *"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security.*
Proceedings of ACM Human-Computer Interaction 6, CSCW2, Article 269 (November 2022), 34 pages. `https://doi.org/10.1145/3555159` — presented at the 25th ACM Conference on Computer-Supported Cooperative Work and Social Computing

This document details the findings of the initial survey and interviews with families, conducted in the second half of 2020.

Publications relating to Chapter 5

Sarah Turner, Jason R.C. Nurse, Shujun Li (2021). *When Googling It Doesn't Work: The Challenge of Finding Security Advice for Smart Home Devices.*
In: Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2021. IFIP Advances in Information and Communication Technology, vol 613. Springer, Cham. `https://doi.org/10.1007/978-3-030-81111-2_10`

Sarah Turner, Jason R.C. Nurse, Shujun Li (2021). *When Googling It Doesn't Work: The Challenge of Finding Security Advice for Smart Home Devices.*
Poster: Seventeenth Symposium on Usable Privacy and Security (SOUPS), 2021, USENIX. `https://www.usenix.org/conference/soups2021/presentation/turner`

This paper and poster presented the findings of the cyber security information review.

Sarah Turner, Jason R.C. Nurse, and Shujun Li. 2022. *"It was hard to find the words": Using an Autoethnographic Diary Study to Understand the Difficulties of*

Smart Home Cyber Security Practices.
In Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI EA '22). Association for Computing Machinery, New York, NY, USA, Article 34, 1–8. `https://doi.org/10.1145/3491101.3503577`

This paper detailed the findings of the autoethnographic diary study. In particular, it focused upon the use and success of the method and the ways in which practitioners could benefit from applying it to their own work or research context.

Papers relating to Chapters 6 and 7 are being drafted at the time of thesis submission.

1.4 Chapter summary

In this chapter, an overview of the thesis topic is presented. There is prior research on how people care about the cyber security of computers in the home. On the contrary, research into the cyber security of home IoT devices, rather than their use, adoption, or privacy considerations, is far less present. Specific groupings of households, in particular parents and children, are also not studied in isolation. In relation to parents and children and digital technology, research has typically focused on how the Internet is used and discussed. This presents a research gap, which is the focus of this thesis: what is the reality of the levels of understanding, management of, and discussion around cyber security for home IoT devices within families in the UK? The chapter then defined the research questions (RQs) arising from this initial framing and the contributions that the thesis makes. It then sets out the organisation of the thesis and the parts of the thesis that have already been published.

Chapter 2

Literature Review

This chapter explores the background and academic literature relevant to the topic, based on — but significantly expanded from — an initial literature review, undertaken in January 2020, which served to frame the RQs posed in the previous chapter. In particular, the literature set out below provides several different angles considered in the subsequent chapters of the thesis and shows gaps where the RQs fit. First, it is important to understand why the harms posed by home IoT devices are considered, and indeed have been shown to be different to that of computers in the home, and from using the Internet. Without this understanding, the importance of engaging with families in relation to this specific type of device may be difficult to understand.

Continuing from the introduction to home IoT devices in Chapter 1.1, Section 2.1 explores the research explaining the difference in harms related to home IoT devices compared to the Internet as used more traditionally in a computer and some implications for users. The differences in harms is particularly important when considering the way in which families have previously been researched in relation to the management, use, and discussion of digital technologies. Families as a whole have largely been researched in relation to the ways in which they live with the Internet. Section 2.2 considers how the management of digital technologies within families has previously been researched.

Section 2.3 considers adults and children's understanding of how IoT devices work and their understanding of and exposure to cyber security knowledge. These types of research are typically done independently — adults and children individually, and, even where households are considered, the interaction between parents and children are rarely considered.

Finally, Section 2.4 gives an overview as to the types of interventions, both technical and non-technical, that have been proposed by prior research as means of mitigating the problems arising from the various issues that multi-use of home IoT devices, children's use of technologies, and maintaining appropriate levels of cyber security and privacy raise.

2.1 The different harms of home IoT devices

When surveyed, academic and industry participants with expertise in the security of IoT devices considered that there is a high potential for crime, exploitation, risk to physical safety and loss of personal control emanating from IoT devices (Tanczer et al. 2018). Loi et al. (2017) has bucketed the potential security risks to IoT devices into four categories, which are: attacks on confidentiality of data;[1] attacks on integrity of data;[2] attacks on access control and availability; and"reflection" attacks — where infected devices may serve to attack other networks.[3] Blythe and Johnson (2019) suggested that a lack of policy and technical intervention may facilitate a "crime harvest", where crimes targeted at the individual (burglary, sex crimes) or a societal level (such as political subjugation) will become more common. A recent review of the literature (Buil-Gil et al. 2023) found that much academic research focusses on privacy in relation to home IoT devices rather than cyber security (a theme that will be found throughout this chapter); in particular, hacking, malware, and denial of service (DoS) attacks are less frequently considered in the literature. Technological measures for these problems are suggested much more frequently than "social prevention", meaning that academic research is more likely to try and solve a specific problem than address potentially socio-wide issues of understanding and mitigation. Storytelling and scenarios are also helping to continue to try to conceptualise the potential issues that home IoT may raise, particularly in relation to children: the physical harms that may occur as a result of playing around with an Internet-connected device were explored as a scenario in Knowles et al. (2019). Despite being science fiction, Doctorow (2019)

[1] For an example involving Amazon's Alexa, see Statt (2018).

[2] For a recent example involving Amazon's Ring, see Paul (2019).

[3] For an example of the Mirai botnet, see Trend Micro (2017); Griffioen and Doerr (2020).

provides a realistic scenario in which children learn how to hack their families' Internet-connected devices to allow them to cook, primarily, significantly cheaper food, without any understanding of the severity of the consequences, both legal and otherwise, of doing so.

Furthermore, with device interfaces typically absent (Geeng and Roesner 2019), app-based control of home IoT devices introduces risks of inequality of use and access, whether intentional (Chatterjee et al. 2018; Markwick et al. 2019) or otherwise (Slupska and Tanczer 2021). Data flows into and out of home IoT devices are prevalent, and users can potentially give away details of their daily movements due to the ways data changes during periods of (in)activity (Tolmie et al. 2016); users may be relatively powerless to make any changes to organisation tracking. Mohajeri Moghaddam et al. (2019) found that a significant percentage of the data generated by popular streaming and smart TV services was tracked to facilitate behavioural advertising, with users unable to take meaningful steps to turn off such tracking. Even if given tools to reduce data flows, they may also end up not using them, despite finding the data interesting (Seymour et al. 2020).

As a relatively nascent technology, users often find that they have to take things into their own hands to get the result they want in their home. As explored by Manandhar et al. (2020) and Cobb et al. (2020), IoT devices are often purchased to link with other physical devices or other pieces of software. In both cases, the use of smart hubs and interoperability tools (such as IFTTT)[4] has been shown to be poorly considered from a security perspective, with users being able to program connections and activities either not considered by the smart hub's designers, or being able to use devices to generate data in publicly available and accessible software (such as open Slack channels or open Google Sheets). Research by Rostami et al. (2022) found that, for users who thought that they may have been hacked, the uncertainty over what was happening was the prevailing feeling — and it was also the case that, as this research was based on user posts on Reddit,[5]https://www.reddit.com/ users may not have had anywhere more formal to turn to in such an uncertain time. Recognising the fact that participants may look for measures over the Internet, other research has found, again using Reddit, that users' attitudes to security and privacy advice may evolve over time, as they

[4] `https://ifttt.com/`

[5] `\protect\relax\unhcopy\strutbox`

become more familiar with the technology — and is influenced by the prevailing sentiment in the subreddit, which may not be in the user's best interests (Li et al. 2023). This suggests not only that the potential harms of home IoT devices are very different from those of the Internet on a computer, but also that users struggle to understand how to use the devices securely.

2.1.1 Threats and mitigants discussed in relation to home IoT devices

As a relatively new technology, there is, perhaps, more speculation than actual lived experience when it comes to the threats that home IoT devices pose. The academic literature tends to focus on specific technical attacks that have been researched and tested in a laboratory, or similar setting (see, for example, Yan et al. (2022); Anthi et al. (2021); OConnor, Jessee and Campos (2021)), and as such consider specific harms as a result of carrying out the attack. Based on this, two systematic reviews of the literature provide an overview of the harms that have been considered in the literature: Blythe and Johnson (2019) and Buil-Gil et al. (2023). From these, general ideas of threats can be drawn, as presented in Table 1. They include several types of device misuse, ranging from the accidental misuse by those with access to the device, to malicious use for tracking, overriding control functions, or denial of services. The conclusions of this academic work are typically technical in nature, suggesting means of strengthening attack surfaces (Hariri, Giannelos and Arief 2020) or allowing for more robust design practises (Yan et al. 2022).

Alongside academic work, there are examples of industry papers and news articles that explore certain threats and harms associated with home IoT device use (with some examples listed in Table 1). News stories typically provide specific examples of a harm being realised (e.g. Liu (2018)), rather than describing generic threats — this, however, is not the case when a vulnerability is being reported (Toulas 2023): in this case, the impact of the found vulnerability often has to be described in terms of possible threat. Industry papers also tend to pose theoretical threats, often in conjunction with a product that mitigates some of the issues described (a phenomenon that will be further discussed in Chapter 5). Chang

(2019), writing for a cyber security firm specialising in endpoint detection, provides a series of compelling threats arising from the integration of IoT devices into the home, including, again, attacks against devices that can make purchases, that can take actions to cue or command, that can map out floor plans or otherwise surveil home occupants.

Where news stories and industry papers often differ from the academic papers exploring specific harms as described above is in the offering of potential measures for users. It is important to note that, in many cases, providing measures as academic papers do, to improve the inherent security of devices through design and development, is an extremely important and necessary part of improving overall cyber security of home IoT devices. However, it does show the relative powerlessness of users to mitigate some of the threats that devices may pose. However, news stories and industry papers are typically focused more on the user than the organisation making the devices, and so may sometimes offer examples of cyber security methods that might make for a more robust smart home. This is also true of explanation and advice pages written by government agencies or consumer bodies (such as National Cyber Security Centre, UK (2019); Laughlin (2021)).

In summary, table 1 lists out possible home IoT device threat types extrapolated from the harm categorisations used in Buil-Gil et al. (2023) and Blythe and Johnson (2019). The table gives examples of academic and news or industry reports on harms linking back to the general threat. In some cases, security measures that can be implemented by the user are suggested. These suggestions, in the majority of cases, come from the news or industry reporting: they typically include the use of, for example, strong passwords and multifactor authentication wherever it is possible to do so — device, companion app, router — understanding and controlling device settings to avoid unexpected use, turning off or limiting device use, and segregating devices on a guest network.

Table 1: Examples of threat types and possible user-based mitigation explored in academic research and news or industry reporting

Threat described	Example of threat	Academic investigation	News or industry reporting	User-based mitigation suggested
Misuse of processing capabilities for external harm	Using home IoT device as part of a botnet	Lyu et al. (2017)	Nokia (2023)	None given
Tampering with physical access control	Smart lock cannot be opened or locked	Fernandes et al. (2017)	Winder (2020)	Update software
Various parts of voice activation process are used maliciously	Malicious smart speaker skills cause unwanted activity (e.g. interference with the home network, additional recording)	Yan et al. (2022)	(Micom Lab 2022)	Use profiles Turn off automatic purchase Turn off device
Inappropriate or unexpected device use by individuals in the home	Purchase of unwanted items	Shank et al. (2023)	Liu (2018)	Turn off automatic purchase Use profiles Delete device histories Unplug device
Control of device by external third party	Forcing a home IoT device to act in ways that cause damage or danger to home or individuals within it	Hariri, Giannelos and Arief (2020)	Chang (2019)	Know devices on network Change default passwords Update software Use guest networks Discussion
Service denial/restriction	Home IoT device functionality is restricted or entirely unusable	Anthi et al. (2021)	Ludlow (2022)	None given
Malicious access of device app	The companion app to the home IoT devices is hacked leading to access to the device settings and controls	OConnor, Jessee and Campos (2021)	Toulas (2023)	Guest network Access codes or passwords for devices or related apps Multi-factor authentication Update software
Tracking activities of users/stalking/ profiling/surveillance	Details about daily routines gleaned from home IoT device activity	Hodges (2021)	Riley (2022)	Profiles for devices Multi-factor-authentication Blocking recording functionality
Data theft	Interception of data stored on or shared with devices by third parties	Lee et al. (2016)	Waugh (2023)	Access codes or passwords for devices or related apps Multi-factor authentication Update software

2.2 Management of family digital technology use

A significant proportion of the research undertaken on family use of digital technologies focusses on the Internet and social networks, much less so on home IoT device use. Although not the focus of this thesis, there are lessons to be taken from the way parents and children use the Internet and social networks.

Shin (2015) discussed that, in general, parents consider access and use of the Internet to be a positive thing, so there is a balance to be performed in providing appropriate access, without exposing children to inappropriate content or other related dangers. However, when interviewed, parents erroneously considered the potential risks posed by the Internet to their children as those to be faced in the future and therefore took minimal actions to act proactively to discuss online safety with their children in the present (a finding echoed in Kumar et al. (2017)). There is also a suggestion that parents believe that they are "above average" when it comes to keeping their children safe online (Blackwell, Gardiner and Schoenebeck 2016), and therefore underestimate the degree to which their children can engage in risky online behaviour (Byrne et al. 2014). A 2022 report based on surveys of 3,808 teenagers in the EU found that just under half (47.76%) had engaged in some form of criminal behaviour (of any sort) online (Davidson et al. 2022). Wisniewski et al. (2017b) showed that this may be exacerbated as a result of a lack of interaction between parents and teenage children — not only do parents avoid the enabling mediation that might prepare children for managing online risks, but children tend not to raise instances where they have encountered risks to their parents, and feel that their parents disproportionately tell them what they cannot — rather than can — do online (Blackwell, Gardiner and Schoenebeck 2016). More recent work (Alsoubai et al. 2022) furthered this, suggesting that the Internet will necessarily be a place of experimentation for adolescents and, as such, the question should not be whether an activity is "risky" or "safe", because activities online are as nuanced as offline behaviours. As such, the ability for parents to discuss the harms associated with use of the Internet — in all its forms — is more important now than ever.

However, parents simply do not understand enough to feel comfortable with what their children are doing, or how to manage it appropriately, or by themselves, often relying on external support or older siblings (Nikken and de Haan 2015).

Cranor et al. (2014) discussed how, for teenagers, parents struggle with the need to exhibit trust to foster maturation and independence — but consider that their children need far less privacy than this trust should afford in the online, or digital, realm than in real life. Sorbring and Lundin (2012) found, that more successful parent-child interaction required knowledge of what the child is doing online. However, research of families (with children aged 10-15) in Norway, Quayyum et al. (2021) found that parents struggled online with keeping control of their children's Internet activities and understanding what they were doing online. Their children did not necessarily have the understanding of what bad things could happen to them, and so their parents struggled to find an appropriate balance between trust and control. The most recent findings of the EU Kids Online project found a significant proportion of "reverse mediation" in certain countries — where children help their parents understand digital technologies (Smahel et al. 2020). Although children from the UK were not included in this survey, it suggests some aspect of a generational gap and a lack of ability for parents to guide their children effectively.

Children also find frustration in parents who do not adhere to the guidelines they themselves put in place (Blackwell, Gardiner and Schoenebeck 2016). Hiniker, Schoenebeck and Kientz (2016) found that families that all adhered to specific rules around the use of digital technology (for example, no phones at the dinner table) kept to such rules more easily – similarly, Ko et al. (2015) showed that the setting of communal rules around the use of digital technology made all family members more likely to adhere to the rules around usage.

Although there is not a huge amount of research dedicated to how parents and children interact with home IoT devices, lessons can be learnt from similar technologies, such as those that allow location tracking. In the years before the mainstream adoption of IoT devices in the mass market, research around the use of location-based services within family groups began to show the issues arising from inequality of data access, and its potential damage to trust (Ur, Jung and Schechter 2014; Yao et al. 2019b; Ferron et al. 2019). Mancini et al. (2011) considered that having access to location data of family members might actually help to fulfil a mothering role, although the balance of controls needed to ensure that this was not taken advantage of, or open to misunderstanding or abuse might actually make family members more vulnerable than if the same technology were to be used between those with less close relationships. Boesen, Rode and Mancini

(2010) reported that although the use of location-based services saw an increase in the compliance of children, this was largely attributable to an unfair change in power dynamics, and one child interviewed commented that he “felt like a prisoner” due to lack of autonomy. Gabriels (2016) argued that this lack of autonomy actually damages self-reliance, and compliant results should not be taken as an indicator of the value of monitoring communication.

Little research explicitly looks at the privacy and security issues that IoT devices create when used by both parents and children in a single location. Ur, Jung and Schechter (2014) looked exclusively at home-entryway surveillance measures, used by both parents and children. It found that although — as with both location-based services and broader Internet use — parents agreed that their children should have privacy when it comes to the setup of such devices, when it comes to the setup of a prototype home entryway surveillance system, parents gave their children the least possible privacy, reasoning that they “had nothing to hide”. Kilic et al. (2022) used an “ideation card game” with the participants to examine the limits of collaborative data management at home. Although between adults, and not parents and children, they discovered that individuals living in the same home veered between feeling uncomfortable about the possibility of people tracking their movements and actions via their data and also not being bothered because of the perceived triviality of much of the data generated.

Much more prevalent is research into multi-use by any group: such research may be beneficial to consider in the context of families, despite the potential for difference in knowledge and capability levels and power dynamics in particular. Yao et al. (2019b) looked at the issues that arise from having IoT devices in a home that is used by outsiders to the family, for example, in a rental home or in a play-date situation. In these situations, the “bystanders” expected a certain level of control, when questioned, either over the way the device worked in their presence, or limitation as to the amount of information the devices collected about them. Crucially, however, this is subject to the “bystander” recognising and understanding the device in the first place and having the power to make the request. Thakkar et al. (2022) found that, while users and bystanders had some common requirements around privacy in common, bystanders were significantly more worried that having a higher requirement around privacy than the user might result in awkwardness or disruption of social norms. Bernd, Abu-Salma and Frik (2020) reported that nannies working within a family context did not consider themselves to have enough power in the relationship with parents — their employers — to ask for the switch off of smart surveillance systems. The research by Windl and Mayer (2022) looked at bystanders with personal relationships and found that the stronger the relationship between the bystander and the device owner, the more potential privacy issues arise from home IoT devices are reduced.

2.3 How adults and children perceive IoT and associated aspects

2.3.1 Perception of Internet of Things devices

Despite the suggestion that the IoT is ubiquitous within society (with a recent industry survey suggesting 81% of the UK population had some knowledge about smart homes (techUK and GfK 2022), fairly recent research — Cannizzaro et al. (2020) — found that among surveyed UK adults, only around half were aware of the terms "Internet of Things" or "smart home". This may point to the fact that knowledge is rapidly growing and is being formed by the adult population in the UK at present. Even where adults understand what devices are, Abdi, Ramokapane and Such (2019) found that individuals tend to lack correct mental models of how devices work, leading to inappropriate control mechanisms. This lack of appropriate mental models has also been shown in children: Pancratz and Diethelm (2020) asked secondary school children to draw their understanding of the computing systems involved in, *including*, a robotic vacuum cleaner and found that the children misunderstood how elements of the systems connected together. Kilic et al. (2022) found that, in asking participants to consider how devices data could be viewed by people other than themselves, a significant minority could not conceptualise, for example, that anyone other than a malicious intruder (a hacker) would be able to see such data.

Strengers et al. (2019) found, in line with earlier work (such as Rode (2010)), that increasing the use of technology at home can actually serve to reaffirm traditional gender roles — men are more likely to undertake the maintenance of devices (so-called "digital housekeeping") as a significant household chore, in place of existing chores. It has long been commented upon that digital technologies are typically considered the preserve of men, with women needing to “catch up” in their understanding of how such devices work (Rode 2011). Research has indicated that this can naturally continue to IoT devices: Boesen, Rode and Mancini (2010) and Geeng and Roesner (2019) found that men were more likely to bring devices into the home, often because they appear fun. Interestingly, more recent research from Cannizzaro et al. (2020) suggested that, in their UK-based survey group at least, women were actually catching up with men in their purchase of domestic IoT products; they argue that this may be due to a desire to use such devices to reduce domestic chores, although it is not clear to what extent using these devices is successful in achieving this. An increase in purchasing may not be quite the same as de-gendering the use of such devices, though: Furszyfer Del Rio, Sovacool and Martiskainen (2021) found, through surveys and focus groups in the UK, that men and women showed gendered attitudes toward home IoT devices, with men still maintaining the stereotypical role of the “driver”, and women more likely to use devices to facilitate cooking, housework or learning. What this research did notice, however, was that these stereotypes did not dominate as much amongst their younger participants, perhaps suggesting a slow movement away from such stereotypes, perhaps as individuals become acquainted with technology from a very young age.

There is a growing body of research on how children interact with conversational agents. Although conversational agents are very specific devices, the research on the whole shows the similarities and differences with which children approach interacting with digital technologies. Beneteau et al. (2020) found that parents used conversational agents to, among other things, further parenting goals; but in an earlier paper, found that familial interaction with devices was often difficult because the device could not interpret the child’s input (Beneteau et al. 2019). Druga et al. (2017) noted that the majority of children experienced “challenges” in getting conversational agents to understand them, although they remain persistent in trying to make the interaction work (Cheng et al. 2018). As with the Beneteau et al. (2019) paper, communications strategies, and scaffolding methods (using adults to model language and ask the questions) were required to get the device to respond.

In the case of conversational agents, children show an inability to understand whether the device is animate or not (Xu and Warschauer 2020), and determine that the devices are “smarter” when they provide answers to their questions (Druga et al. 2017). This ties into the comments from parents recorded in McReynolds et al. (2017) that not only are toys designed to motivate the child to use “adult devices”, but the restrictions placed on the technologies used within Internet-connected toys often see children putting them aside to use devices such as Google Home or Amazon Echo instead. Despite this, there appears to be less research done into other common smart devices (such as Smart TVs, vacuum cleaners or thermostats) and children’s interaction. Getting an understanding of how children perceive and interact with such devices would be beneficial to get a better understanding of their mental models around how such devices work — and how they differ from those of adults, and from their use of the Internet and social media on computers and smartphones.

2.3.2 Perception of cyber security

There is little prior research on how children deal with cyber security in IoT devices explicitly, or the risks posed by ubiquitous devices over using the Internet through a computer. Quayyum, Cruzes and Jaccheri (2021) pointed out that only two of the 56 studies they reviewed on raising awareness of cyber security for children raised financial loss (a possible risk of compromise of home IoT devices), with the majority focussing on online safety. Kumar et al. (2017) explored the mental models that children aged 5-11 had around privacy and security in relation to Internet use. Although they found that the children were able to develop some strategies for control (such as providing false information), they relied heavily on their parents for support. Lamond et al. (2022) also found that the research focused on the knowledge of children and not the skills or competency required of children to carry out good cyber security practise. As discussed in Section 2.2, this is problematic, as parents struggle to understand technology themselves.

Research with older children shows that they are not only interested in learning about privacy issues (Yap and Lee 2020), but that they feel strongly that they should be given their own privacy, whether from family or corporations (Coleman et al. 2017). This is backed up by research such as Dowthwaite et al. (2020), which found that teenagers were not easily able to conceptualise the amount of data collection currently done online, and, despite typically becoming more interested when given engaging prompts for discussion, they could not understand threats beyond those that would affect them personally. Experiences of parental control are less frequently considered in research than how adults react to their privacy being overlooked, with location-based research being a possible exception (Czeskis et al. 2010; Boesen, Rode and Mancini 2010; Mancini et al. 2011; Vasalou, Oostveen and Joinson 2012; Gabriels 2016), as discussed in Section 2.2.

Cyber security risks are considerably less prominent in sociotechnical research on IoT devices than privacy risks, and in instances where they are it is typical for cyber security not to be defined (Mazurek et al. 2010; Floros et al. 2012; Minkus, Liu and Ross 2015; McReynolds et al. 2017; Steinberg 2017; Ahmad et al. 2018; Brosch 2018; Garitaonandia, Karrera and Larranaga 2019). Nicholson et al. (2021b) found that although children had decent knowledge of core cyber security principles, they did not necessarily reflect this in their actions, something also seen in Pencheva, Hallett and Rashid (2020), where teenagers showing technical competence online actually demonstrated significantly insecure behaviour in school at least. Garitaonandia, Karrera and Larranaga (2019) went into detail about the cyber security risks that children had faced, pulling data from the 2011 EU Kids Online survey. Many surveyed children had faced cyber security issues, from data breaches to viruses: the same issues were considered both for computers and smartphones. IoT devices were not considered separately in this survey. In the most recent version of the EU Kids Online Survey (Smahel et al. 2020), information from 15 countries on data misuse found that an average of 15% of children had been affected by a virus or spyware in the past year, although the risk of this happening increased with age and was significantly higher in some countries, compared with others. Although focussing on areas other than cyber security, Blum-Ross and Livingstone (2020) describe two instances in which parents are unaware or unable to remove viruses from desktop computers that had been purchased to facilitate their child's interest in digital technologies. The implicit suggestion in both cases was that the virus had rendered the devices useless due to a lack of ability to remove it or a lack of ability to find appropriate support.

Little research provides any detail on how parents and children discuss cyber security, particularly in the context of IoT devices in the home. Pencheva, Hallett and Rashid (2020) considered how, even if children were to turn to teachers or parents for support, adults may have less knowledge than the child. Muir and Joinson (2020) talked about how both parents and children use not only each other, but also a range of other trusted friends and family members to discuss and handle cyber security problems. Interestingly, there seems to be a complicated relationship between both sides when seeking advice from friends and family members. Nthala and Flechais (2018) explored how family members with technology expertise struggled with ongoing requests for support from others. Nicholson et al. (2021a), found, however, in a study aimed at training older adults to support peers with cyber security issues, families of those trained also reported benefiting from the advice when surveyed. Importantly, but perhaps unsurprisingly, Morrison, Coventry and Briggs (2021) found that receiving support from family members actually led to poorer individual long-term results, in older people, as it created a relationship of trust with someone else understanding and acting on the problem at hand.

This makes it important, therefore, to ensure that parents, whilst supporting their children in their cyber security setup, do not do it all for them. However, parents seem to consider themselves responsible for their children's safe and appropriate device use. Prasad, Ruiz and Stablein (2019) found a majority of parents felt they could only trust themselves to protect their children's privacy (and not device manufacturers); Boffi (2020) provides the example that parents were unwilling to allow children free-range to a device that allowed them to place telephone calls to others because they could not control misuse.

2.3.3 How do adults and children learn about digital technology risks?

Bada, Sasse and Nurse (2015) discussed how national cyber awareness strategies often fail. In particular, in assuming that people are motivated by similar things — especially fear — the messages often fall flat. Reasonable cyber security often requires effort and understanding to implement appropriately. It is often the case that understanding is lacking (for example, Wash (2010) and Forget et al. (2016)), and the effort is so great that Herley (2009) has argued that it is, in fact, rational to ignore cyber security messages.

The current UK cyber awareness schemes include Cyber Aware[6] from the National Cyber Security Centre (NCSC), who also have specific websites with information for individuals and families, and also for smart devices. This shares a space with other organisations, such as Get Safe Online,[7] a public-private partnership that provides information on several current cyber security issues. Similarly, financial institutions offer guidance about cyber security to their customers, promoting government guidance and resources on stopping fraud and scam-based activities.[8] On a global scale, there are non-governmental organisations that produce detailed documentation from several perspectives, from minimising the risk of surveillance from third parties (including governments),[9] or assisting those who are suffering domestic abuse or coercive control through digital technologies.[10] In addition to this, certain technical journalism outlets have also created their own guides to "Not Getting Hacked", as Vice refers to theirs (Motherboard 2018).

Consumer advice bodies, such as Which? in the UK, provide reviews of specific devices and occasionally run broader sectorial guides. These bodies have taken particular interest in the last few years in the safety and security of Internet-connected toys, with the Finnish consumer protection body in particular releasing a report provocatively named *#toyfail* to highlight their concerns (Forbrukerradet 2016); concerns that have since been followed up by Which? in the UK (Laughlin 2021) and Consumer Reports in the United States (Fowler 2018). As home IoT devices are increasingly popular, these bodies — for example, Which? — put out general advisory notices on how to stay safe when purchasing or selling products (Laughlin 2022), and also more specific news stories when problems are found (Laughlin 2020). Mozilla has, since 2017, maintained its "Privacy Not Included" guide,[11] which gives product reviews of home IoT devices, focussing upon their

[6] `https://www.ncsc.gov.uk/cyberaware/home`

[7] `https://www.getsafeonline.org/`

[8] For example, HSBC's customer page on cyber security sends readers to the UK government's "Take Five" toolkit (`https://takefive-stopfraud.org.uk/`), a scheme to combat financial fraud.

[9] For example, the Electronic Frontier Foundation's Surveillance Self Defence guidance (`https://ssd.eff.org/`).

[10] For example the global charity Chayn (`https://www.chayn.co/`), and UK-based charity Refuge (`https://refuge.org.uk/i-need-help-now/how-we-can-help-you/secure-your-tech/`): both offer support on the use of digital technologies in abusive relationships, and support for more "traditional" abuse cases.

[11] `https://foundation.mozilla.org/en/privacynotincluded/`

"creepiness". The guide was started because "[i]t is often difficult for consumers to get clear, concrete information from companies about the security and privacy of their connected products" (Mozilla Foundation 2021).

In addition to the various awareness mechanisms provided for adults, in England, there is a national computing curriculum that has been in place since 2013 (Department for Education, UK Government 2013). With teaching requirements throughout the school life of a child, it focusses on building an understanding of computational thinking as well as digital literacy. This, too, is a crowded space — although there are specific curriculum-based aims per Key Stage for children, these are supplemented, again, with materials and schemes from various bodies and public-private initiatives. For example, there are NCSC's Cyber Sprinters[12] game and activities for 7-11-year-olds, and the more targeted CyberFirst scheme[13] for 11-17-year-olds with an interest in cyber security. The UK Safer Internet Centre,[14] a partnership of three charities focussing on children and safe Internet use, provides significant resources to anyone wishing to help children (from ages 3-19) to "stay safe online"; they also partner with private institutions (such as financial services firms) to give training sessions to children in schools. Furthermore, charities such as NSPCC[15] and Childnet[16] offer support to parents and guardians. The big tech firms are also present in this space, notably Google, with their "Be Internet Legends" campaign.[17]

The curriculum and, as a result, the guidance provided by organisations such as the UK Safer Internet Centre is heavily focused on dangers that translate from non-digital safeguarding concerns. At the youngest age, Key Stage 1, children are expected to "use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the Internet or other online technologies" (Department for Education, UK Government 2013). This idea is constant throughout the four Key Stages (representing an entire school education, from 5 to 18 years); the oldest school age children are expected to "understand how changes in technology affect

[12] https://www.ncsc.gov.uk/collection/cybersprinters

[13] https://www.ncsc.gov.uk/cyberfirst/overview

[14] https://www.saferinternet.org.uk/

[15] https://www.nspcc.org.uk/keeping-children-safe/online-safety/

[16] https://www.childnet.com/

[17] https://beinternetawesome.withgoogle.com/en_uk/

safety, including new ways to protect their online privacy and identity, and how to report a range of concerns" (Department for Education, UK Government 2013).

The security focus is on protecting personal data for safeguarding reasons — be wary of developing relationships online ("stranger danger") and do not use the anonymity of the Internet to bully or harm others ("cyberbullying"). These concepts are taught alongside how to code and some understanding of how the Internet and other digital technologies work. Blum-Ross and Livingstone (2020) found, however, that there is a fundamental disconnect between learning at school and any learning that takes place outside of school (at after-school activities — even those that take place on school grounds — or through individual endeavour). This disconnect, they argue, is to the detriment of not only the family, but also the school in being unable to tie lived experience to the curriculum.

2.4 What measures have been proposed?

2.4.1 Technological interventions

The calls for technological measures for privacy problems, in particular, created by technological development, are not new. It seems common for calls for the modification of existing digital technologies, through, for example, the change of the user interfaces to be more explicit about how the use of a digital technology may affect others (Mancini et al. 2011), the introduction of nudging tactics to promote privacy awareness (Cranor et al. 2014; Minkus, Liu and Ross 2015; Wisniewski et al. 2017a; Quayyum, Cruzes and Jaccheri 2021), or the better control of personal data sharing, whether through obfuscation or notification of data use (Yardi and Bruckman 2011; Manches et al. 2015). There is also recognition of a need for "fine grain" or "contextual" privacy settings (as originally set out in Nissenbaum (2010)) — the need for technology to recognise that individuals may take a very nuanced approach to the use of their information, based upon many factors (for example, the time of day, the location, the device or the people they are with) (Mazurek et al. 2010; Abaquita et al. 2020). Coles-Kemp, Jensen and Heath (2020) argued, however, that this notion of contextual privacy may not serve the needs of people in a "post-digital" society, and there should be a shift to understanding what the risk factors for the individual are that need to be addressed at any time, an argument repeated by Alsoubai et al. (2022). This is particularly the case for vulnerable groups and should be kept in mind when approaching security matters at home. Ur, Jung and Schechter (2014) showed, for example, that parents and children disagreed on the retention period for images from a home entry surveillance system — crucially, children, the vulnerable group, believed that a shorter retention period would balance security with their privacy appropriately, compared to their parents.

Many pieces of research have investigated the feasibility of technological interventions in helping home users understand how their smart home operates. There has been a focus on trying to visualise data flows arising from IoT devices as a means of informing the user about the quantity of data produced (Zimmermann et al. 2019; Coulton and Lindley 2019; Seymour et al. 2020). Zimmermann et al. (2019) found, from a small study, that user knowledge decreased as a result of prototype use (although it is unclear whether this was an anomaly due to the small number of participants). In other cases, notably, the Aretha system prototyped in Seymour et al. (2020), users found the visual guide to data flows interesting and informing, but it did not prompt them to use the built-in firewall controls. The authors suggest that this could be because there are simply too many "data destinations" for the user to understand and act upon.

Other research has looked at prototype technologies that manage home security risks by providing control to an individual (or individuals) (Nurse, Atamli and Martin 2016; Nthala 2019). Nurse, Atamli and Martin (2016) found that, although users initially grasped the concept of the interface, users themselves were lacking the ability to determine logical threats; there was also a concern that the proposed device would simply not scale. Nthala (2019) created a system that allowed individuals to control devices within a home, regardless of who the individual is: whilst this may help solve many day-to-day issues where users draft in third-parties to help resolve problems, it raises bigger concerns in terms of the ease with which such a system could be abused.

The problems of multi-use of devices — and thus the need for sensitive control of the risks of such devices, has not been explored in prototyped technologies, as noted in Pattnaik, Li and Nurse (2023). This is particularly pertinent when considering the power dynamic of parents and the part that independence plays in child maturation. Research on existing technologies, including parental control devices and location-based services, shows that although parents and children believe that there may be benefits to such technology, it is more likely to erode trust as a result of the ease with which it can be misused (Boesen, Rode and Mancini 2010; Czeskis et al. 2010; Gabriels 2016; Vasalou, Oostveen and Joinson 2012). Calls for the participation of children in the design process are frequent, to ensure that diverse use cases and capabilities are considered (Czeskis et al. 2010; Boesen, Rode and Mancini 2010; Ko et al. 2015; McReynolds et al. 2017; Yao et al. 2019b). However, measures for help children navigate the smart home, such as detailed in Madani et al. (2018), are still designed with a view to the management of children's activities by the parent, rather than a joint effort to create an agreed-upon outcome. Both Ko et al. (2015) and Park and Lim (2020) showed that when families discuss how they want to use and control digital technologies, they come up with results that are significantly more egalitarian between parents and children, and are more likely to be adopted by the entire family.

2.4.2 Non-technological and sociotechnical interventions

The academic literature sets out that users need to understand the digital technologies that they use better, to minimise the privacy and security risks that they may pose – see, for example, McReynolds et al. (2017); Nuhla et al. (2018); Brosch (2018); Garitaonandia, Karrera and Larranaga (2019); Yao et al. (2019b); Goulden (2019).

Within a family context for home IoT devices, this would necessarily mean that both parents and children, as users, should be expanding their knowledge. Not specifically in relation to home IoT devices, but digital technologies in general, there are several calls for schools and governments to play an active role in the promotion of knowledge to minimise potential Internet-based risks (Shin 2015; Nikken and de Haan 2015; Ahmad et al. 2018; Nuhla et al. 2018); recent research from Norway shows that such an intervention, provided by schools, benefits both children and parents (Quayyum et al. 2021).

It is difficult to know how to increase the knowledge of those who are not in full-time education. Parkin et al. (2019) investigated discussing the issues of device use at the point of in-person purchase, and Vetrivel et al. (2023) looked at the prevalence and usefulness of Amazon reviews providing security and privacy advice; Blythe and Johnson (2018); Emami-Naeini et al. (2020) have argued for, and produced, prototype labels that detail key information about IoT devices, similar to nutritional advice labels. These can only truly work with greater understanding of the way the devices work in the first place.

Several articles have started to report more experimental play-based methods for engaging participants, both as a means of promoting the design of devices intended for groups, including families (Christensen, Skovgaard and Petersen 2019; Verweij 2019; Park and Lim 2020; Bourdeau et al. 2020). Serious games have also been used in the privacy and cyber security space, both for research purposes (Williams, Nurse and Creese 2019; Shams, Arachchilage and Such 2020) and as tabletop exercises for those in industry (Frey et al. 2019; Hart et al. 2020; Gondree and Peterson 2013; Denning, Shostack and Kohno 2014). Kritzinger (2017) suggested a gaming approach to attract all stakeholders — from children through to the government — into increasing the "cyber-safety" cultures within South African schools. Online games and play have also been successful in increasing awareness within university environments (Innocenzi et al. 2018). This is particularly important when considering the knowledge scaffolding that may be necessary when teaching children about cyber security (Zhao et al. 2019), or involving them in design processes (Superti Pantoja et al. 2020).

Several pieces of research show how user-centred design (UCD) can be used — both for exploring how users may like to have cyber security measures designed for them (Fassl, Gröber and Krombholz 2021), but also in exploring what security measures users might value in home IoT design or labelling about such measures on packaging at point of purchase (Yao et al. 2019a; Emami-Naeini et al. 2019b). However, this method does not necessarily translate into industry: Chalhoub et al. (2020) found that, in practise, security is considered a technical, not user-centred problem, in the design of home IoT systems, which makes the complexity and difficulty of use compound as the number of devices in a home increases. Furthermore, where there have been calls to consider children to be considered "protagonists" (Iversen, Smith and Dindler 2017) and "users" (Druin 2002) when it comes to design, UCD provides a welcoming environment for children to explore and provide useful feedback during iterations of the design process, sometimes alone or in school settings (Metatla et al. 2019) and sometimes with parents and caregivers (Koumpouros and Toulias 2020). Although a common finding of UCD – particularly in cyber security research – is that it must be bounded by expert knowledge that ensures that user input does not cause unintended consequences (Yao et al. 2019a; Fassl, Gröber and Krombholz 2021), UCD can provide for a better result for users. For example Ylizaliturri-Salcedo et al. (2018), found that, in addition to building a functional child tracking strap, the children involved proposed ways to make the strap more fun for them, by introducing stickers and other artefacts to make the strap more playful and unique.

2.5 Limitations and gaps in the literature

In performing the literature review, there are some limitations that are important to call out, as they impact the research detailed in this thesis.

The academic literature does not necessarily distinguish between online safety, privacy, data protection, and cyber security when discussing the way individuals use devices and the Internet. The fundamental concept that seems to arise uniformly is the importance of the strong password. The literature on IoT devices, and how people perceive them and their risks, is heavily based on privacy. This is, of course, a significant concern that requires attention, but other aspects of cyber security are less considered in the sociotechnical literature. For example, the literature rarely reviews the understanding and intent behind why individuals protect their Internet-connected devices the way they do, or what the main risks are beyond inappropriate content. Home IoT devices are designed to collect data from all around; there are additional issues of consent, power relationships, and knowledge that are not fully explored in the literature. Physical security is also rarely mentioned, despite ongoing findings that some smart devices are sold with questionable physical safety, as well as more well-reported cyber weaknesses (Laughlin 2020). This is an issue as people become dependent upon home IoT devices for the management of their day-to-day lives, but run the risk of having the device fail, or provide insights into their lives that facilitate fraud or burglary, for example. This is important because there will likely be similar levels of confusion when discussing these topics with research participants; it seems likely that they may expect that cyber security measures are relatively uniform, rather than recognising that some may be more relevant for certain situations than others.

In addition to this, clear guidance on how users should consider cyber security for home IoT device use is largely absent. Technical academic literature typically focuses on very specific vulnerabilities or harms, with narrow and specific measures, in many cases — and this leads to technical recommendations for product developers and designers, not users. There is little in the literature that specifically looks at what users should or can do to improve the cyber security of the home IoT devices that they use, and there is a focus on known existing harms, rather than wider threats for consideration (beyond the aspect of loss of privacy). The most useful type of literature for user-based cyber-security measures is news articles or industry reports, both of which do not necessarily have the rigour expected of academic publications. This is a gap that arises, as Buil-Gil et al. (2023) notes, because there is, in general, a lack of information on harms, given the nascent state of the home IoT market. Without these experiential data, much of the work to be done to help users protect themselves relies on conjuring up theoretical threats upon which reasonable cyber security measures can be used.

Table 1 lists out a number of types of threat and possible cyber security measures, as considered in the literature. Although further discussed throughout the thesis, in particular in Chapters 5 and Chapters 6 and 7, there are additional cyber security measures that may be relevant in addition to experienced harms or suggested by national security organisations, such as NCSC, NIST, FBI or consumer organisations such as Which?. As the research documented in Chapters 6 and 7 explores, there are a range of potential cyber security measures that could be used, depending upon the setup of the home and the devices in question, ranging from ensuring strong and unique password use and management to turning off devices or obscuring cameras. This is a gap that is explored during the thesis, but Table 2 sets out a proposed list of cyber security measures that a user may want to put in place in relation to their home IoT devices, based upon the combination of academic research, news articles, industry reports, and recommendations from government agencies and consumer bodies (for further details as to where these recommendations come from, see Appendix I).

Table 2: Proposed cyber security steps users should consider taking in relation to home IoT use

Cyber security measure	What does it achieve
Access codes for device applications	Allows a layer of protection where a home IoT device can be controlled through an app on a smartphone/tablet
Access code on smart phone	Although not directly used with home IoT devices, the use of a passcode on a smart phone will reduce the likelihood of compromise of devices apps in the instance that the phone upon which the apps is on is stolen
Back up devices	Allows for minimal loss of device use should there be a hardware fault, or should the data on the device be otherwise compromised
Change router password	The router is the gateway to and from the Internet in a house; having a strong, unique password will make it harder to compromise
Delete device history	As devices and their related account store significant amounts of data, deleting data you no longer want used (including when you finish using the device) minimises the data that could be compromised
Factory reset	When you stop using a device, factory reset it to ensure that any relevant data on the device itself will no longer be available
Family discussion about device use	Allows for rules about appropriate device use to be negotiated and understood; expectations managed about use
Multi-factor authentication	Allows a layer of protection where a home IoT device can be controlled through an app on a smartphone/tablet
Password manager	Although likely not directly used with home IoT devices, the use of a password manager facilitates stronger passwords, which can be used to protect accounts and apps linked to home IoT devices
Profiles for device use	Allows for minimisation of attacks done through voice recognition; allows for segregation of content and control
Review devices on network	Allows for removal of devices that may not otherwise have been noticed on the network
Strong, unique password use	Using a strong, unique password - such as one formulated using the NCSC's "three random words" strategy - makes accounts harder to compromise
Tape/cover over cameras	This stops anyone seeing through a camera when they should not
Turn off automatic purchases	Stops individuals purchasing items using previously given financial information unless the account holder gives permission
Unplug devices when not in use	If the device is not plugged in, it cannot collect data or — more fundamentally — be used at all
Use antivirus software	Although it is likely not to directly protect home IoT devices, the use of antivirus on computers and other relevant devices on the same network may help to minimise compromise through malware.
Use automatic software updates	Ensure the device receives important software updates (which can relate to patching vulnerabilities) without any active participation for the user
Use guest network	This allows for the segregation of devices to avoid infection on one network spreading to the other(s), or users on one network gaining access to the devices on another

2.6 Literature review conclusions

The literature review highlights many areas in which further research should be considered and supports the RQs laid out in Chapter 1.2.3.

The predominance of qualitative research focuses on families and the use of the Internet, social media, and smartphones. This is a useful starting place, but as home IoT devices can pose significantly different threats to users — and bystanders — there will be clear differences arising that need further consideration.

It seems clear also from the literature that people do not engage with cyber security unless there is a need. Home IoT devices seem to occupy a strange space where, one day in the future, they may control various aspects of people's lives, but right now they are more used for frivolous activities and do not necessarily play more than a small part in people's lives. Parallel to this, there is a lack of education, both for adults and children, as to what IoT devices at home are, how they work and what controls they may have. This is concerning, as it could allow for a situation where devices slowly become more necessary and expected, but the requisite knowledge to manage them is not freely available. Academic research around potential cyber security is often focused on specific technical concerns, and the novelty of the devices means that a broad set of harms upon which to base examples of good cyber security is limited. There needs to be a deeper understanding of how to fill that knowledge gap — both in terms of the education that is needed for adults and children, but also in terms of the delivery of that information.

It is also clear from the literature that technological measures can, in some cases, modify behaviour change and understanding positively for at least the duration of the research. UCD appears to be beneficial in producing more widely considered outcomes — although it is unclear how well the designs that are generated from such sessions map well into actual measures. Indeed, on the other hand, technologies prototyped to help individuals visualise and understand how data flows in the household have had marginal success at best, with participants either not fully using the intervention methods because they were too overwhelming, or actually realising they understood less as the testing period progressed. From these results there must be a concern that asking the individual to insert themselves into managing such complex and confusing technologies is potentially the wrong solution. There is also the risk that, when designing for families, the inequalities arising from the inability of children or other family members to control the home IoT device will always be a factor that cannot be mitigated against.

This chapter has addressed the reasons for why certain topics have been chosen for the thesis. The following chapter will explore the how, looking at the research methods used, the reasons behind those methods and the practical implications of performing the research.

Chapter 3

An Overview of Methodological Choices

In this chapter, the methodological approaches used in the thesis are discussed. This chapter should be considered as an overview of the techniques applied. More details will be provided at the appropriate places in subsequent chapters. This chapter builds upon the previous chapter in explaining how the RQs that have arisen from the gaps in literature are addressed using the chosen research methods, and why.

The chapter begins with a brief overview of the research methods undertaken. It goes on to give an explanation of the research philosophy and the subsequent approach to methodology taken, along with a reflection on the beliefs and perspectives brought to the research by the researcher. It goes on to describe the qualitative measures generally applied throughout the thesis, and then, more briefly, those quantitative aspects that were applied where appropriate. As the thesis focusses upon a demographic group (that of the family) that cannot possibly be said to be homogeneous, the assumptions taken about such a group when performing the research are then detailed out. Finally, there is information on the ethical process undertaken for the relevant research steps and the impact that the COVID-19 pandemic has had on the research process.

3.1 Overview of the research undertaken

3.1.1 The individual pieces of research undertaken

The research presented in the research is spread across four chapters (Chapter 4 to Chapter 7); there are four distinct pieces of research that have been carried out to address the RQs set out in Chapter 1.2.3. The following chapter breaks down the research process: the different steps within the research process of each piece. This section, along with Table 3, will give a brief overview of the shape of the research itself, along with prior examples, where possible, of where similar research methods have been used in previous research and a justification for each method and the combination as a whole. The research comprising this thesis displays a range of methods that try to meet the user group — in this case, the family — the level of awareness they have, at the time when the research was performed. Initially, this was by discussing and asking questions about their experience, then exploring the ways in which they may encounter cyber security information and times in which the issues may arise. Recognising the paucity of chances to encounter home IoT device security, and the lack of understanding, the final piece of research allowed families to have their say in creating a game that would present cyber security messages in a way that felt enjoyable and impactful to them.

The first piece of research (detailed in Chapter 4), uses a survey and interviews to explore questions about the use of home IoT devices, and understanding of cyber security at home of those families in the UK who participated. The use of surveys and interviews is a common way to obtain feedback on a topic: combining the two allows a combination of the breadth of the response around the questions (as further considered in Section 3.3.1), and depth (with interviews of 25 families), as further considered in Section 3.3.2. Interviews and surveys are commonly used together as a research method in HCI research (Chhetri and Genaro Motti 2022; Tabassum et al. 2020): here, this approach was used as an initial entry point into the topic — surveying and interviewing the user group being researched in the thesis allowed for an understanding of where the research should go next.

Table 3: Overview of research and methods

	Date period of research	Participants involved?	Data types collected?	Method(s) of analysis
Interviews and Surveys	Summer – early Autumn 2020	25 families 553 valid survey responses	Interview transcripts Survey data	Reflexive thematic analysis (transcripts) Quantitative analysis (survey data)
Website Review	Autumn – Winter 2020	n/a	Website content and meta-data	Content Analysis (both qualitative and quantitative)
Autoethnographic Diary Study	Late Summer – Autumn 2020	Researcher and immediate family	Diary entries	Reflexive thematic analysis
user-centred design	2021 – Summer 2022	23 families 100 control survey participants	Interview transcripts Video recordings	Reflexive thematic analysis

In the event, two pieces of information emerged from the interviews and surveys which determined the two following pieces of research (as well as informing the final piece of research). Surveys and interviews showed that when participants felt like they had a problem or needed to learn more about their home IoT device, they would google it.

There is no guarantee, however, in that situation that the person searching would have the right vocabulary or find pertinent results. The research in Chapter 5 uses content analysis of websites to review this information directly, allowing an understanding of the ease of finding appropriate information and whether the information found was from trusted resources and easily implementable (as discussed further in Section 3.3.3). Content analysis of the value of online cyber security information has been performed before by Redmiles et al. (2020) and also Li et al. (2023).

The other piece of information arising from the interviews and surveys informing the research detailed out in Chapter 5 was that families rarely talked about cyber security of home IoT devices or, furthermore, considered that such a discussion was needed at home. This consideration posed a question to the researcher: how do you address the family group on the topic of cyber security of home IoT devices if they do not even consider it in daily life? What aspects of the researcher's expectations and assumptions about the use of home IoT devices and ensuring their security is driven by an interest in, and knowledge of, cyber security itself? What can realistically be expected of a family using home IoT devices? And how might that affect how families can address the need to learn more about cyber security of home IoT devices? These questions — coupled with the period of COVID-19 lockdowns — led to an autoethnography (as explored in Section 3.3.4). Autoethnography has been used before, in HCI settings, to help researchers understand their practice as a user, rather than an expert (O'Kane, Rogers and Blandford 2014; Malinverni and Pares 2016), although this is the first time that this research method appears to have been applied to cyber security.

The final piece of research, as documented in Chapters 6 and 7 explore how families can expand their awareness (advancing through the cycle described in TTM, as described in Chapter 1) about cyber security of IoT devices at home using a board game. The use of board games in cyber security research is not new (Frey et al. 2019; Haggman 2019), although this is the first time that this has been used with the user group of a family to learn about home IoT devices. The piece of research had two aspects: user-centred design (as described in Chapter 1), to allow for the creation of a game that would be modified by participating teams throughout the process to create a more playable and enjoyable final product. The other aspect looked at the way in which the game helped participants extend their awareness about cyber security of devices in the home, and whether they were subsequently more likely to make changes to their cyber security set up at home, compared to a control group. Control groups are periodically used in human-centred cyber security research (Albayram, Liu and Cangonj 2021), although measuring the effectiveness of using a cyber security board game using a control group seems to be novel to this research.

The remainder of this Chapter will explore the methodology and its implications in more detail.

3.2 Research philosophy and approach

It should be clear that this thesis takes at its core a qualitative research approach as a means of understanding the actors and actions being investigated. Although specific research activities (notably the survey) may tend to a more quantitative approach, in general, the overall approach fits well with Cresswell's definition of qualitative study as an "enquiry process for understanding a social or human problem, based on building a complex and holistic picture, formed with words, reporting detailed views of informants and conducted in a natural setting" (Creswell 1994).

Theoretically, the choice of methods stems from an *inductive* viewpoint: a focus on observations and findings generating theories and understanding, rather than modifying previously held hypotheses. As such, research generally uses *interpretivism* as its epistemological lens, with a starting point of understanding human behaviour "as a product of how people interpret the world" (Bogdan and Taylor 1975) and, by extension, *constructionism* as its ontological framework (Clark et al. 2021) — in particular, it feels important to recognise the constantly shifting understanding and experience of the use of devices not only at an individual family level, where household members grow and change, but at a societal level, where opinions, legal frameworks, and technological advances can alter over short periods of time. This recognition will allow for framing the research and its findings in such a way that it can withstand such shifts.

3.2.1 Epistemological framing: interpretivism and positivism

Interpretivism

Although the pieces of research undertaken in this thesis will not be further described in terms of their epistemological lenses[1] beyond this section, it is important to recognise the complexity of placing qualitative research into the broader academic field of Computer Science, even if the research sits within HCI (Human-Computer Interaction) or usable security. Research, such as the pieces undertaken in this thesis, is necessarily interpretivist in its epistemological approach. Roughly speaking, interpretivism starts from the understanding that individuals cannot be studied in line with scientific models: This study requires interpretation from the researchers to unravel the reasoning behind the thoughts actions and understandings of the individuals involved (Clark et al. 2021; Chandler and Munday 2011); that a person's reality is subjective, not objective. Although this is an extremely broad piece of terminology, there are aspects both of the *hermaneutic* and *phenomenological* views of interpretivism used in this thesis. Hermeneutics is an approach to interpretivism that has its basis in philosophical views that are far beyond the scope of this work and is applied in an extremely broad range of areas (Svenaeus 2012). The key aspects that are applied in elements of this thesis are the importance of considering the embedded meaning of the evidence produced from a piece of research. In particular, this means considering evidence holistically, rather than semantically, which has impacts on the approach used for thematic analysis (see Section 3.5.1). Another aspect of hermeneutically based analysis is the importance of the role of meaning, and the need to recognise the importance of ambiguity and contradiction in the evidence as it arises (Magee 2011). The majority of the research in this thesis primarily uses a hermeneutic epistemological lens to consider the implications of evidence.

[1] The understanding used to explore how knowledge is gathered and framed.

Although hermeneutics and phenomenology have significant amounts in common – particularly when considered without a deep philosophical lens – it is important to recognise the role of phenomenology too, as a framing of this thesis – especially in relation to the autoethnographic work and the necessary process of reflexivity as a means of creating more robust outcomes from thematic analysis. Phenomenology encompasses the recognition of the importance of subjectivity in research that involves understanding human behaviour: "see[ing] things from that person's point of view" (Bogdan and Taylor 1975). This is an extremely important framework in a field such as usable security, where, despite decades of effort, users still struggle to implement suggested best practices. Approaching the research in the thesis by recalling the requirement to see the user's point of view — rather than through the eyes of the researcher — is vital for nuanced findings, as explored in depth in Chapter 5.3.

Positivism

Positivism is typically considered the converse of interpretivism — although, just as with interpretivism, it covers a broad church of definitions, here we will broadly consider it to be the use of methods used in natural sciences to study people and social reality (Clark et al. 2021). In particular, there is focus upon the objectivity of results, and confirmable outcomes as a means of knowledge generation, that there is one single truth, ultimately: and thus can be considered to be broadly aligned with more quantitative methods of data collection. As discussed in Blandford, Furniss and Makri (2016), quantitative methods and a broadly positivist approach have an extremely important role in HCI research, allowing for specific analysis of hypotheses related to people's reactions to and engagement with technologies. This thesis, being interdisciplinary in approach, sits amongst several potential academic areas, and as such, has to be cognisant of those tests and data treatments that are considered as being sufficiently robust. Although, as seen in papers such as McDonald, Schoenebeck and Forte (2019) there is ongoing consideration as to the appropriate use of overtly positivist methods as a means of evidencing robustness of method and quality of the outcome of research, steps such as inter-rater reliability, use of hypotheses (where relevant for the data), and control groups have been used in relevant places in the thesis to provide the currently expected levels of scientific rigour expected in these fields.

3.2.2 Ontological framing: constructionism and objectivism

The discussion of the ontological framework[2] here will be shorter than that of the epistemological framework that preceded it. Specifically, the ontological framework that this thesis has is one of constructionism (sometimes referred to as constructivism), the understanding that things are as they are because people have always — and continue to — shape things based upon their perceptions and actions (Clark et al. 2021). This is in contrast to objectivism, where things are external facts that are beyond a person's influence to change. Although one may argue that the concept of a family could be considered to be objectivist, in that it is an understood structure that, generally speaking, has understood norms (there will be adult(s) and child(ren), there will be hierarchical norms where the adult(s) will be responsible for setting boundaries and supporting the child(ren) as they grow), in a world of fast-changing technological advancement, this does not feel like an appropriate framing. In particular, relationships between adults, children, and the technology in their homes alter every time a new device is added, or is shaped by the decision to not include them. Digital technologies, too, have shaped relationships between parents and children over time – as can be seen, for example, from the modification of the suggestion by Livingstone that enabling mediation, once an improvement upon the parental mediation model that preceded it, does not go far enough and should be replaced with methods that allow the agency of the child to play a role (Blum-Ross and Livingstone 2020). The knowledge building that this work argues needs to be done to improve cyber security awareness is obviously something that requires shaping based upon the perceptions and actions of those who take part.

3.2.3 Researcher perspective

As well as the theoretical underpinning of the research, it is important to understand some of the perspectives and the background of the researcher. Assumptions and decisions made about the research methodology and analysis – in particular, reflexive analysis, as described in Section 3.5.1 – may well reflect the core assumptions and beliefs of the researcher. It is worth noting that the researcher is a mother of two young children (aged 3 and 6 at the start of the research process).

[2] The study of how things are, and have come to be.

Her experience of parenting children, therefore, does not extend out to older children. This could prove problematic in several respects: she could assume that her own children reflect the normal behaviour or understandings of children of that age, whilst not fully understanding the rationale for the actions of older children. Parents, too, are not a monolith, and so care has to be taken to respect the approaches of others. Similarly, family structure is far from set in stone, and the researcher's own family set up is relatively culturally traditional for the UK — a family with heterosexual parents living together in a single home — again, possibly making it difficult for the researcher to fully grasp the fluidity and complexity of some familial arrangements.

The researcher lives in London with her family (her two children and husband, who is a software engineer), and has lived in urban locations in England her entire life, ensuring an expectation of functioning services, such as a stable connection to the Internet. It also belies an England-centric understanding of how public services, laws, and regulations work, which may be different in the devolved nations (and certainly, internationally). She and her husband have — aside from periods of full-time education — always both worked in full-time roles, allowing for a degree of financial freedom that may not be shared by many others. Despite this, they do not engage with home IoT devices (beyond those mentioned in Chapter 5): they are not early adopters of technology, preferring only to use technology when it solves a predefined need. There are no other blockers to owning home IoT devices: they own their own home and have discretionary income that could be spent on such devices. Their close friends and family are also not necessarily early adopters of technology. This means that the researcher is not and is not surrounded by people who are immediately interested in exploring the novelty or potential usefulness of home IoT devices.

The researcher has an academic background in the humanities and social sciences, with a focus (at different times, in different qualifications) on law, people and organisational management and public policy. Her professional background is in financial services; in particular in the application of regulation to activity undertaken by the organisations she has worked in and the assessment of conduct and reputational risk. These endeavours underline a core aspect of the assumption behind the research: that, within the UK, there is an expectation that public policy through a combination of law and regulation will protect citizens where there is the potential that they may suffer harm (as is true in financial services, for example). This comes with a linked expectation that when organisations create products or services that have the potential to cause harm, they will have adequate and meaningful risk management and controls in place to adhere to the legal or regulatory requirements of the jurisdiction in which they are selling their product or service. The researcher believes that the digital technology sector is such a vital aspect of society today that certain aspects around consumer protection may require regulation, in similar ways to financial products and services that are available to consumers. This is a belief that makes the researcher uncomfortable with the expectation of "responsibilization" of cyber security (Prior and Renaud 2023), given the complexity of understanding appropriate actions. These views, of course, may reflect in the nature of recommendations made arising from the research within this thesis.

3.3 Research methods used

This section will look briefly at the methods used in each piece of research that forms the thesis at a high level. More details will be provided at the start of each piece of research. Table 3 gives an overview of what is discussed below.

3.3.1 Surveys

Surveys are used in Chapters 4 and 6. In general, surveying participants lends itself to a more quantitative approach, which is not necessarily in line with the research approach discussed in the previous sections. However, the interplay of qualitative and quantitative methods (sometimes referred to as "mixed methods") is often considered beneficial for several reasons, as detailed in (Bryman 2006), and seen in practise, for example, in Tabassum et al. (2020). Firstly, the numbers of participants involved in interview processes are often relatively small, meaning there can be questions around the generalisability of the results that come from it. Being able to conduct a survey on the same themes – as is done in this thesis – allows for the opportunity to provide a wider *validation* of the findings of the interviews, based on that wider sample size. In turn, the use of a survey allows the provision of an element of *completeness* to the research that may be missing through just interviews alone: in this case, the surveys complementing the interviews allow not only for a slightly wider range of questions about device use to be uniformly asked, but provide a wider geographical range of people, to allow for, arguably, a better representation of families in the UK.[3] Both of these aspects, hope, help lend an element of *credibility* by combining the results of surveys alongside qualitative results.

3.3.2 Semi-structured interviews

Interviews are used in Chapters 4 and 6. The approach used for interviewing the participants was that of the semi-structured interview. This method requires a predetermined framework of questions — which can be a mixture of open-ended and closed-ended questions — but that allows the researcher to probe areas of particular interest or relevance as they arise within individual interviews (Clark et al. 2021). This method of interaction with participants is extremely common in the HCI field, as it allows a broad range of discussion and feedback on technical matters, regardless of the age or level of skill of the individuals interviewed (for example, Tang et al. (2022); Huang, Obada-Obieh and Beznosov (2020)). The flexibility available in semi-structured interviews was particularly important when interviewing family groups: different families have different lived experiences and may find certain aspects of the topic more or less pertinent to their lives. Children, in particular, may not respond well to a structured interview, where they are required to answer a set list of questions without deviation; planning for some organic deviation from the questions considered generally important in the semi-structured interview plan was vital to ensure ongoing participant engagement.

3.3.3 Website Review

The website review is explored in Chapter 5. The website review is a somewhat different piece of work compared to the other elements of the research in this thesis. It uses content analysis (as will be discussed further in Section 3.5.2) to review information that is freely available online. This can be a valuable source of data (Kim and Kuljis 2010), and allows for reflection upon what, in this case,

[3] Although it should be noted that the participants in the survey were not specifically selected as a demographically representative sample of the UK population.

users may find to assist them online. This adds rich additional context to the semi-structured interviews in particular, as it allows for a contrast between what interview participants believe they can take from online sources as against what is actually there when analysed against particular criteria. This is an increasingly used form of analysis in this field, for example, Blythe, Johnson and Manning (2020); Turner et al. (2021); Rostami et al. (2022) all use online data to understand what is available for users that may want to find more information about security issues online.

3.3.4 Autoethnographic diary study

Autoethnographic diary study is used in Chapter 5. Chang (2016) describes autoethnography as autobiographical writing that "combines cultural analysis and interpretation with narrative details", with Ellis, Adams and Bochner (2010) describing it as "an approach to research and writing that seeks to describe and systematically analyse personal experience to understand cultural experience". Its inclusion as a research method here is particularly relevant in terms of the cultural exploration of the acceptance of the wider use of digital technologies and the difficulty that the average home user has had with implementing cyber security measures over a period of decades. The reflexivity of autoethnography is a useful way of understanding the researcher's place relative to the research topic and can help with understanding biases and preconceived notions before performing analysis on qualitative data.

However, such works can be challenging to understand, as they typically raise concerns in relation to the independence, objectivity, and generalisability of the method (Rapp 2018). However, the collection of personal thoughts and reflections on a topic for a period of time by a researcher can serve as a lightweight research method that, done well, gives the ability to provide nuanced insights that can outweigh the obvious lack of generalisability (Eschler 2016). Malinverni and Pares (2016) used autoethnography to determine the importance of how personal values shape their work as researchers, leading to more considered and grounded future research, particularly when working with users in design activities.

Within Chapter 5.3 the research is referred to as an "autoethnographic diary study". This is because the researcher wanted to test the value of using a diary study as a potential next step in the thesis, whilst doing it only by herself. Hyers (2018) described the diary study as being “distinct for its capacity to capture phenomena of interest on a regular basis, in context and over time”, and so could be used as a means of getting participants to self-report life experiences in a predetermined way, when they experience something of interest — Bolger, Davis and Rafaeli (2003) discussed the usefulness of this method to capture differences of experiences within the participant group, reporting activities much closer to real-time than in an interview (Sheble and Wildemuth 2009): whilst not possible in a sample of one, as in this piece of research, there could be promise for a future piece of research as a means of understanding RQ3.

3.3.5 User-centred design

User-centred design methods are used in Chapter 6. User-centred design (UCD) is a widely used term in HCI research, covering a range of methods which focus on designing for, and including users in the design of, computer systems, tools and so on. Given the breadth of this definition, there is a wide range of potential activities that can be labelled UCD, from involvement in only usability testing of a created product or service through to involvement at every stage, from initial design considerations through to the creation of a finalised product (Abras et al. 2004).

Hodges-Schell and O’Brien (2015) detailed out the benefits of including non-designers in the design process, including demystifying the design process (which can lead to more open feedback) but, more importantly here, giving the non-designers or stakeholders ownership of the ideas underpinning the design of the product. UCD, in this thesis, is introduced in the final stage of research, the intervention, as a means of engaging the researched group — families — to provide design opinions on the gameplay, design, and enjoyability of a board game, as well as feedback on clarity and understanding of the concepts raised in the game (a process also seen in Emami-Naeini et al. (2019b)). The intention behind this is that a board game designed with the people it is supposed to target should end up being more appealing, something that speaks to them more directly, if their voices are heard about what works or does not, for them, in the design process.

Gulliksen et al. (2003) used existing theory and their own research experience to adopt 12 key principles for successful UCD. As that work mainly considers UCD in organisational settings, not all are relevant here, but some key aspects are central to the intention behind the approach:

- *User focus* — the users' goals, tasks and needs should early guide the development
- *Active user involvement* — representative users should actively participate, early and continuously through the entire development process and throughout the ... lifecycle [of development]
- *Evolutionary ... development* — the development should be both iterative and incremental
- *Prototyping* — early and continuously, prototypes should be used to visualise and evaluate ideas ... in cooperation with the end users
- *Evaluate use in context* — the design should be based on specific design criteria and critical usability goals
- *Explicit and conscious design activities* — the user interface and interaction design are of undisputed importance for the success of the system — for users, the interface is the system.

This last point is particularly important to consider here: as described in the original conception of UCD (Norman 1986): " the purpose of the system is to serve the user...the needs of the users should dominate the design of the interface, and the needs of the interface should dominate the design of the rest of the system." Obviously, in this case, this must be applied to the context of a board game, not a piece of software; however, the message to take from this is that the delivery of the information about core cyber security methods and their application — the things that the game needs to do — must be provided to the user in ways that work, primarily, for them. As considered in Mitchell et al. (2016), the use of UCD can also be beneficial to the generation of ideas, as it gives a more holistic perspective on the problem to be solved.

There is an immediate tension, however, and one that is discussed in various pieces of research using this technique: that users, although extremely important as the end target of a product, often do not fully understand the nuances and complexities of what they are assisting in the design of. This has been seen in cyber security-based UCD experiments, where non-expert users propose measures that either do not take account of the full range of measures at their disposal, or — perhaps more importantly — present other security or privacy problems that the user cannot contemplate (Yao et al. 2019a): experts must be able to override user suggestions that do not work (Fassl, Gröber and Krombholz 2021). This is seen, outside of HCI, in other research areas where UCD is used for serious game design with children in particular: in healthcare and teaching settings, experts had to ensure that information and pedagogical values were correct, even where children may have wanted to make changes (Ouherrou et al. 2023; Sparapani et al. 2023). This is a tension that will be further explored in Chapter 7.

3.4 Data collection and preparation

There are four pieces of research that constitute the entirety of this thesis. Each generated significant amounts of data, which was subsequently analysed in ways that are further explored in the methodology section for each piece of research.

This section will describe at a high level the overarching aspects of data collection and preparation.This will be discussed in depth to explore the methods used to preserve the privacy of participants and the accuracy of the collected data.

3.4.1 Storage of data

The storage of data will be discussed first, as it remains the same across all pieces of research, regardless of the type of research undertaken. Data, once collected, were stored in encrypted files on the University of Kent cloud storage system (OneDrive). The encryption keys were kept solely by the researcher and were required for each access to the relevant file. It was considered that the University's OneDrive storage would be the most appropriate place to store the data primarily, given that storing files in the cloud — and in particular, a cloud service located within the EEA and/or UK to comply with GDPR requirements — allowed for a level of redundancy, should the researcher's computer fail. However, once all data were anonymised (where necessary, depending on the research), the files were stored, again, in encrypted files, on two external hard drives by the researcher to provide further levels of redundancy. These hard drives were kept locked at the researcher's home. The hard drives were kept at the researcher's home as the research was carried out at various stages of the COVID-19 pandemic, meaning that access to the university campus and infrastructure was, in large part, not consistently available until after the majority of the research had been carried out.

3.4.2 Survey data collection

Surveys were used in the research documented in Chapters 4 and 6. In all cases, the platform used to host the survey remained the same (Jisc's Online Surveys),[4] and was used primarily because of the stated GDPR compliance of the platform and ISO 27001 certification, providing assurance as to the privacy and security of stored data. Where relevant, participants were sought through the Prolific platform,[5] a platform that allows the researcher to specify the particular inclusion criteria needed for participants, and the ability to set appropriate levels of pay for participation. In this thesis, the representative pay level used to ensure that participants were paid fairly for their work was the Real Living Wage,[6] which was raised over the period of the thesis. The 2019/2020 year had a rate of £9.30; by the 2021/2022 tax year, this had increased to £9.50. At no point in the process did any participant provide a name or other identifying characteristics, with the one exception of opting in to receive further information about subsequent participation in either the interviews or gameplay sessions. Even then, the communication was done through Prolific's messaging platform, allowing for ongoing anonymity for participants if desired, although many participants interested in participating in this way subsequently provided the researcher with an e-mail address for easier communication.

There is always a risk, when using online participant platforms such as Prolific, that the survey responses will not be meaningful or even real, given the anonymity of the participants and the inability of researchers to otherwise validate it. Two steps were taken to minimise this problem, as far as possible: the

[4] `https://www.onlinesurveys.ac.uk/`

[5] `https://www.prolific.co/`

[6] `https://www.livingwage.org.uk/what-real-living-wage`

first, already mentioned, was the payment of a fair amount in relation to the work being done; the second was the employment of attention checks in surveys carried out with Prolific participants; two attention checks were included as part of the survey. Although potentially a contentious method of measuring concentration and therefore care taken to answer accurately (Gummer, Roßmann and Silber 2021; Kung, Kwok and Brown 2018), it was decided before the analysis that participants who failed both attention checks in a survey would have their answers removed from any further analysis.

3.4.3 Tools for survey data analysis

Once the surveys had been completed, the researcher had to collect the data from two places: the survey answers from Jisc's Online Surveys and then the demographic information about the participants from Prolific. These two datasets could be combined using the Prolific ID provided in both. The data sets were analysed using a combination of tools: IBM SPSS and Microsoft Excel.

3.4.4 Interview and video recording

The audio recording formed the basis for both interview processes in the thesis. Additionally, the sections of the gameplay sessions where participants were playing the game were video recorded, in case there were non-verbal actions that needed to be captured and analysed, subsequently. Participants who played the game in person were recorded using a video recorder, angled to capture the board and, as much as possible, not the faces of the participants. Those participants that participated online were recorded through the instance of Microsoft Teams that was used for the session — again, the camera being used was angled away from the faces of the participants, as much as possible, to focus on the board. These video recorded sessions were also audio recorded.

All interviews were subsequently manually transcribed by the researcher using Microsoft Word (allowing for uniformity of the transcripts for use in the analytical tool). Interview recordings were deleted after transcription, although video recordings were kept during the analysis process for the reason described above.

3.4.5 Tools for interview analysis

The transcribed interviews were then subjected to thematic analysis (for more, see Section 3.5.1). This was done in MaxQDA,[7] software designed for coding documents, rather than manually, or without specialist software. MaxQDA is one of a number of potential software solutions that could be used for this work and was chosen simply as a result, primarily, of the researcher's personal preference for it, but also after confirmation that the second coder would also be able to use it. It also allowed for the coding of video and text within the same structure, allowing for easy integration of data collected in Chapters 6 and 7. This software was also used to code the electronic copies of the diary entries captured as part of the autoethnography.

3.5 Methods of analysis

The prior section explained the method of data collection and the tools used for the analysis, both qualitatively and quantitatively. This section will explore the key method chosen for analysing the qualitative data in the thesis, and then provide a brief explanation about the role of quantitative methods in the work.

3.5.1 Reflexive thematic analysis

The primary method of qualitative research analysis in this thesis is thematic analysis (Braun and Clarke 2006). This method allows relative freedom for the researcher to distinguish, refine, and analyse themes in the data. The term is extremely flexible, and following their seminal 2006 paper, which is the starting point for the definition of thematic analysis here, has been restated and refined by Braun and Clarke over the years. In particular, Braun and Clarke (2021) made clear the added importance of reflexivity at the core of the version of thematic analysis they pioneer, which is an important clarification that will be further explored below; it is this restatement that the analysis in this thesis uses, that of reflexive thematic analysis.

[7] `https://www.maxqda.com/`

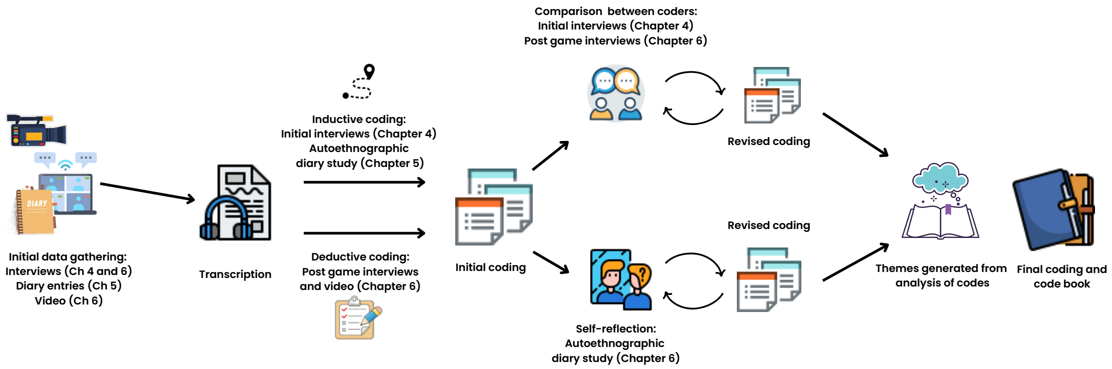


Figure 2: The process of thematic analysis

The theory behind reflexive thematic analysis

Reflexive thematic analysis is a method that offers guidelines, not rules, about how to apply it to a data set. There are four variations that Braun and Clarke lay out in their 2021 book that they suggest should be considered prior to starting — inductive/deductive, semantic/latent, experiential/critical, realist or essentialist/relativist, or constructionist — although analysis for every data set will sit somewhere between one or the other of each, with few being explicitly at one end or the other of the spectrum.

Even within this thesis, there are differences between the variations used. As a general starting point for interviews and opinions, the researcher's decision was that it was appropriate to use *inductive* approaches to creating themes from the data. An inductive approach allows the researcher to approach the data without any preconceived notions as to what the end result of the analysis will be. This helps when, as is the case in Chapters 4 and 5, the intention behind the research is to uncover the themes that are important to gain an understanding of the RQs. Chapter 6 was different, however. When considering specific feedback about the board game and gameplaying sessions discussed in Chapter 6, a more *deductive* approach was used, starting with a pre-determined list of codes to apply to the dataset allowed for a more straightforward improvement process. The UCD aspects required that participants provide certain pieces of feedback to improve the game: the areas of feedback needed were known in advance of the interview and so were used as the codes by which the interview data was coded. In each case, a code book was created, and can be found in Appendices C, G and O. For an overview of how the process worked in the different research pieces, see Figure 2.

Due to the nature of the research, starting from the premise that knowledge and understanding would be low within family groups during the process, it was decided that a *latent* approach to interpreting the meanings of words, phrases, and sentences should be approached, as the expected outcome was that large amounts of uncertainty, ambiguity, and inaccuracies would be captured in the data sets. To use a *semantic* approach would focus more on the words used, rather than the gaps — which would miss out this richness in this case. Similarly, due to the type of exploration performed with families in the work interviewed, most of the analysis was done with an *experiential* mindset. The only place where this differed was in performing thematic analysis on the diary entries for autoethnography, where part of the aim was necessarily to consider the entries in a more *critical* manner, trying to unravel more of the meaning of what the words were saying. It is fair to say, however, that the "theoretical framework" underpinning all the analysis was *relativist* in nature: in order to get to an end-point of understanding the gaps in knowledge, and the potential interventions needed, the analysis had to look to interrogate the realities within the dataset, rather than taking them at face value. It should be clear to see the overlap between these variations and the epistemological and ontological framings discussed above.

Why is the role of reflexivity so important in the restatement of Braun and Clarke's version of thematic analysis? In short, without knowledge of the researcher's biases or opinions that they bring, inherently, to the research, it is very hard to argue about the value of the research because there is no real way to judge the rigour of the work. It could be inherently biased without, or perhaps worse, with the knowledge of the researcher. Considering the impact that the researcher themselves has on the outcome of the work is a non-quantitative way of trying to capture the reliability of the outcome, in such a way that inter-rater reliability may be used elsewhere — and indeed, is in this thesis, for the reasons described in Section 3.2.1. Although not presented in this order in this document, the autoethnography work described in Chapter 5 was an attempt by the researcher to perform a period of reflexive work prior to analysing any of the data sets collected from families.

The practice of reflexive thematic analysis

There are a number of steps to perform the reflexive thematic analysis, which are explained in Figure 2. It is important to note that the process of coding the data is iterative, one where, in particular, the final steps are repeated more than once, and may never feel fully finished. The process of manually transcribing interviews is important, if time-consuming, as a way of getting immersed in the data before starting to code them.

In two cases (the data in Chapters 4 and 6), a second researcher coded the data (the "second coder"). This allowed for the calculation of an inter-rater reliability metric — in these cases Cohen's *kappa* — to give an understanding of the level of (or, rather lack of) subjectivity in the coding process; namely, an ability to confirm some level of repeatability in the process. This is not always necessary in coding-based work, although it is often preferred in Computer Science-based research. In particular, this goes against the principles laid out by Braun and Clarke (2021). In fact, the importance of reflexivity meant that the autoethnographic diary study (Chapter 5.3) had no second coder, a decision supported by a recent reconsideration of the importance of inter-rater reliability in the HCI and CSCW fields (McDonald, Schoenebeck and Forte 2019).

The same researcher second-coded both studies mentioned above. The second coder was a PhD student at the School of Computing, and the Institute for Cyber Security for Society at the University of Kent, with the primary researcher. In terms of research, the second coder also has an interest in understanding cyber security of home IoT devices, but through a more technical, rather than sociotechnical, lens. Being older than the primary researcher, the second coder is mother of a child older than the children of the primary researcher, and has different cultural references, coming to the UK from another country, living elsewhere in England (in a town), with a professional background in teaching computer science to older children and adults. This background is helpful in understanding that there was necessarily a level of understanding of both the technologies being discussed and the potential risks and threats, and also of personal experience of parenting. The differences around parenting older children, interacting more generally with children in relation to digital technologies, and the more technical nature of the second coder's research all added to slightly different approaches that allowed for discussion, based upon these different life experiences, during the coding process.

Coding the data — as mentioned above, using software specifically designed for this purpose — involves reading through the transcripts (or watching the videos, as relevant) in conjunction with the code book. Depending upon the deductive or inductive nature of the process, the code book will either be formed at the start of the process or will evolve as the transcripts are analysed. The relevant sections of the research data are then "tagged" with particular codes. This is an iterative process, particularly in the case of inductive coding, where earlier transcripts may end up needing recoding based upon the findings in the later transcripts, or based upon discussions with the second coder, where relevant. In discussions with the second coder, the researcher would analyse a merged version of the coded transcripts, showing both the researcher's and the second coder's coding, to find areas of disagreement (typically text coded with different codes). These disagreements would then be discussed with the second coder, to understand the reasoning behind the difference, discussing the interpretations of each person, to see if one or other person would come to a place of agreement. It was not necessary to get to perfect agreement — this work has an element of subjectivity — but rather to help gain fullness of understanding from both parties working with the data. When the researcher was working by herself, a similar process was achieved by multiple rounds of coding and seeing if the coding from previous iterations still felt appropriate.

Coding the data is typically the beginning of the thematic analysis process and is the most clearly explained. Once the above-mentioned discussions about coding itself were completed, the less structured process of finding (and where necessary agreeing upon) the themes arising within the data, using the codes as jigsaw pieces, to create a coherent picture, was begun. Having knowledge of all the data (through reviewing it multiple times during the coding process), it is possible to see larger themes that comprise information within several codes. When working alone, this, again, is an iterative process, working to understand how the codes may link together into larger themes for discussion. With a second coder, discussion can be very helpful in solidifying ideas based on the opinions of both coders. In both cases that the second coder was involved in this research, individual reflections of the coded text were discussed together. This allowed both researchers the opportunity to respond to the reflections of the other and test them against their own. Disagreements of opinion could be discussed to find common ground on a set of themes that could then be taken forward for writing.

3.5.2 Content Analysis

It is important to call out the slightly different method of analysis used in the website review (Chapter 5.2). It relies on content analysis to review documents available to individuals when searching for information about cyber security and devices online. Content analysis allows for the rigorous analysis of such documentation, requiring, as it does, a framework to be imposed around the scoping of data collection, the method of collection, and the review process itself (White and Marsh 2006).

It also allows elements of both qualitative and quantitative to be captured, allowing a wide range of conclusions to be drawn about what is said, who is saying it, how it is being said and, crucially, what is not being said (Neuman 1997). Here, as considered by Kim and Kuljis (2010), and seen in papers such as Blythe, Johnson and Manning (2020), the criteria by which the pieces of data are to be considered are initially laid out. In this case, the information collected included not only questions about the information explained in the text but also further pieces of meta-data: for example, who had written the information, when was it dated, and who was the information aimed at? The collation of these data (in a spreadsheet) subsequently provides the basis for analysis not only of the text, but also quantitative aspects as mentioned above — how many articles mentioned a particular topic (or did not), how many were written by which sort of outlets, and so on.

3.5.3 Quantitative methods

Having stated the qualitative underpinning of the majority of this thesis, it is hard to argue that qualitative research, which typically relies on small numbers of research participants and their lived experience, can or should be assumed to be widely representative of entire populations. As such, in order to provide additional robustness to the investigation, where it makes sense, mixed methods have been employed (Clark et al. 2021). Quantitative analysis can provide data on the experience of more people (through survey analysis) and provides methods to determine the connection between and relevance of research findings. In what has been described as an embedded design approach (Creswell and Plano Clark 2007), both elements of quantitative and qualitative research can be used concurrently, and the analysis integrated, to create a single set of more robust findings. This approach is taken in both the initial interviews and the survey work in Chapter 4, as well as the final intervention work in Chapters 6 and 7.

In line with the qualitative nature of the wider work, where data was provided that could be analysed quantitatively, it was categorical in nature: more specifically, nominal variables. This led to two specific treatments of the data: a general use of descriptive statistics, which could provide a level of comparison within a specific variable. When analysing comparisons between groups, however, Pearson's chi-square test of independence for nominal variables was used (Pearson 1900). This test allows us to understand the reported results of each group, based on the expected average result given the sample size and total responses. Much higher, or lower, reported results compared with the average expected highlights the likelihood of statistical significance — that is to say, that the results are likely not due to correlation. Such analyses are reported in the format $\chi^2(\textit{degrees of freedom}, N = \textit{sample size}) = \textit{chi-square statistic value}, p - \textit{value}.$ A high chi-squared statistic value denotes a likely significant result. The p-value was required to have an α of less than 0.05 to suggest statistical significance. It should be noted that the statistical analysis carried out between control and gameplay group is further discussed in Chapter 6: because of a disparity between the sizes of the two groups as a result of resource limitation, there may be questions as to the statistical robustness of the conclusions drawn. As discussed in Chapters 6 and 7, this should not necessarily detract from the findings, given the general picture that the responses from the two groups paint.

3.6 Assumptions made about the family unit in the UK

It is important to recognise that there is difficulty in accurately assessing the very target group of the thesis. A "family " is, in the UK of the 21st century, a term that covers a multitude of arrangements of adults and children in some way or another. It should be noted upfront that the breadth or limitations of the term "family" in this thesis are not defined by researchers, aside from the need to have school-aged children living at home, when recruiting participants.[8] Instead, so as to avoid being overly limiting, participants were allowed to interpret the use of the term as necessary for their situation, with the one exception for co-parented children, as described below.

In their report about the state of families and households in the UK, the Office of National Statistics uses the following definition (Office for National Statistics 2021a):

> A "family" is:
>
> a married, civil partnered or cohabiting couple with or without children, or a lone parent with at least one child, who lives at the same address. Children may be dependent or non-dependent.
>
> "Dependent children" are:
>
> those living with their parent(s) who are either
>
> - aged under 16 years, or
> - aged 16 to 18 years
>
> and who are in full-time education, excluding children aged 16 to 18 years who have a spouse, partner or child living in the household.
>
> "Non-dependent children" are:
>
> those living with their parent(s) and who are either
>
> - aged 19 years or over, or
> - aged 16 to 18 years
>
> and who are not in full-time education and have no spouse, partner or child living in the household. Non-dependent children are sometimes called adult children.

Families can, of course, be significantly more complicated than this definition allows. As a start, Brown, Manning and Stykes (2015) discussed how statistical data on children's living arrangements and wellbeing in the United States

[8] Of course, it should be noted that this is an extremely limited definition of family, as it is not the case that all groups considering themselves as such will have children; this is an important limitation around this research.

ignore the "complexity" of the family by focussing on the link between parent and child — what about situations where siblings may live with different parents, or the integration of half- or step siblings? The 2022 figures published by the UK government recorded 82,170 "looked after" children in the UK (Department for Education 2022). Looked after children are those that have been in the care of their local authority for more than 24 hours, which can see them living in residential children's homes, residential settings like schools or secured units, or in foster homes (National Society for the Prevention of Cruelty to Children (NSPCC) 2022). Foster children can often become part of a family, with specific requirements and differences to be considered. Within the thesis, two families were involved who had a total of three foster children living with them. These children were an integrated part of the families, in one of the families involved referring to their foster parents as "mum" and "dad". However, the foster parents were aware that their foster children must be more protected from certain aspects of digital technologies than their biological children; a sentiment raised a number of times by adult participants in the research who were also teachers.

As families come in all shapes and sizes, the inclusion criteria for participation were kept broad enough to avoid excluding families that did not meet more traditional interpretations. In particular, only one adult and one child were required to participate (with additional requirements on the age of the children in the household during the gameplay session), and it was clarified that although the term "parent" may have been used, it included any adult-child relationship where there was a formal guardian relationship in place. To cover instances of co-parenting, it was decided to set the requirement that children could be included for interview, so long as they spent 50% or more of their average week at home, mostly so that they would have the opportunity to engage with the devices.

An area that we could not directly cover in the inclusion criteria was the assumption that the participants involved would live in households free of domestic abuse or coercive control. Should the researcher have intimated from any comments within any of the interviews or gameplaying sessions undertaken, the assessment made as part of the submissions to the University's ethics committee was that any concerns would be escalated, via the researcher's supervisory team, to the ethics committee for further guidance; or, in the case of the researcher being concerned as to the immediate safety of any of the participants, directly

Table 4: Details of favourable ethics opinions

Research	Application number	Date of receipt of favourable opinion
Interviews and surveys (Chapter 4)	0751920	22 July 2020
Cyber security awareness information review (Chapter 5)	n/a (not research with human subjects)	n/a
Autoethnographic diary study (Chapter 5)	0851920	11 August 2020
User centred design (board game) (Chapters 6 and 7)	CREAG-001_11_2021	7 December 2021

contacting appropriate law enforcement. This was explained to the participants on the research information sheet. Domestic abuse and coercive control in relation to digital technologies at home are significant issues and have been widely and sensitively considered in both academic research (Parkin et al. 2020; Lopez-Neira et al. 2019; Stevens et al. 2021) and relevant bodies in the third sector[9] These work pieces must be considered when recommendations are made as a result of this thesis, although specific findings as a result of this thesis will not incorporate first-hand examples of this issue.

3.7 Ethics considerations

Any research involving human subjects undertaken at the University of Kent requires a favourable opinion from the appropriate ethics committee, in this case the University's Central Research Ethics Advisory Group (CREAG).[10] All research involving human subjects — the initial interviews and surveys, the autoethnography, and the final gameplaying research — were required to complete a full ethics application, requiring full details of the proposed research approach, explanation of, and mitigations to, all potential risks to participants and researchers involved and how informed consent would be sought from participants. For a list of favourable opinion details, see Table 4.

The fundamental aspect of the formal ethics review process is the evaluation of a wide range of documents relating to the piece of research. Typically, this includes detailed explanations of the intention of the investigation and the proposed mitigation plans for any risks that were outlined, along with the intended questions, survey structures, consent forms, information sheets, and any other

[9] These bodies include Chayn `https://www.chayn.co/` and Refuge `https://refuge.org.uk/i-need-help-now/how-we-can-help-you/secure-your-tech/`.

[10] Prior to 2021, this board was referred to as the Faculty Research Ethics Advisory Group.

documentation that the participants would see. Once reviewed, the ethics committee could ask follow-up questions and require amendments until they were satisfied and a favourable opinion secured.

A key aspect of the ethical obligations that researchers have to their participants is ensuring that they understand the potential risks involved in participating in the research. Such risks are typically set out in an information sheet, which is then read by the participant before giving their informed consent to participation.[11] This is more complex when children are involved — not only because the concepts in the information sheets are often complex, but also because they are typically not able to give consent to such data collection themselves.[12] Despite being unable to consent, it is important to ensure that children are informed of what the research entails, and that they are aware of what this means for them, in just the same way as adults (National Society for the Prevention of Cruelty to Children (NSPCC) 2020). In this way, children can be said to have assented to participation, although their parents have formally signed the consent form.

Practically speaking, assent was gained from children through a brief discussion at the start of each research session to ensure that the entire family — both adults and children — were comfortable with the terms of the research. Parents were also provided an information sheet with the full details, which they could use for further discussion with the children if needed. Participants were also made aware that the researcher held an enhanced check from the Disclosure and Barring Service, that they could view or ask further questions about if needed. Parents then signed consent forms on behalf of themselves and any children under 18.

Survey participants were also required to give their informed consent before taking the survey. The information typically given to participants as an information sheet was entered as the first page of the online survey portal, requiring the participant to read before providing consent, by answering a yes/no question asking if they consented based upon the wording in the information that they had just read. Any participants answering no to this question would be sent to

[11] Part of the process of informed consent is letting the participant know that they can withdraw this consent at any time.

[12] As to when they can consent to such collection is contested. Although under the UK GDPR, the age at which children can consent to data collection is 13, the GDPR suggests that the age should be 16. As agreed with the University's CREAG, however, for the purposes of this research, children under 18 were not able to consent independently.

a screen thanking them for their time but informing them that as they had not consented, they would not be able to take part.

3.8 Impact of the COVID-19 pandemic

Although the end result of the research thesis is one with valid and timely findings, it is important to acknowledge that this process was significantly altered by the COVID-19 pandemic, which reached the UK in late February 2020, and has been a fixture throughout the research process.[13] This section will reflect the impact of the pandemic on the thesis, as in some respects, it has made things easier, in others, harder, a finding that has been echoed by other qualitative researchers (Howlett 2022; Pocock, Smith and Wiles 2021; Mikulak et al. 2022).

The requirement for people to stay home or restrict their movements for periods of time, since March 2020 in the UK, has been extremely beneficial for the smart home market, with consumer research finding that the pandemic brought forward purchasing decisions about Internet-connected products such as smart TVs (techUK and GfK 2021). The devices considered in this thesis are now significantly more ubiquitous than before the stay-at-home period, which has been beneficial not only in being able to find interested research participants and materials, but also in maintaining the importance of the research topic. It is for this reason that there has been a confirmatory survey run in 2022 included in Chapter 4, to understand how the market and people's reaction and use of devices have stabilised (or not) as the restriction of movement associated with the earlier days of the pandemic are permanently forgotten.

Work and study from home measures have also made the use of video conferencing an everyday event that even the youngest of children are aware of. This has been very helpful in being able to interview a much wider range of participants with extreme ease, as location was not an issue — undertaking the first round of interviews six months into the pandemic, there was a level of comfort that almost all participants showed with connecting to a video conferencing system to be interviewed. This level of comfort remained true through to the gameplay sessions in 2022, being able to recruit a number of families from a much broader geographical range to play later rounds of the game online without the associated costs

[13] This doctorate began mid-January 2020.

of travel, and so on. This was a particular relief as repeated lockdowns and the emergence of new variants of concern — in particular the Omicron variant in the winter of 2021 — beset the final piece of research with quite a significant amount of uncertainty as to whether participants would even be willing to participate without an online option. It seems like conducting research in their own homes enabled participants to feel at ease, being in their home, and allowed for a flow of conversation. In relation to the interviews, this allowed for a structure where participants could drop in and out after they had answered questions aimed explicitly at them. It also allowed bored or unengaged children (which sometimes happened with children under ten) to leave both interviews or gameplay sessions with relative freedom, without disrupting the parents in the same way as happened in person. In the case of children in particular, this allowed for more freedom when interviewed: they could demonstrate how they used their devices rather than just speak about it — extremely helpful when they may not have had the vocabulary to explain.

Despite the ease with which those families that participated online managed to do so, this must be tempered with the recognition that, despite the ubiquity of the Internet in many people's lives, this does not mean that everyone has equal and appropriate access to it. This has been felt particularly during the period of the pandemic, when children who did not have access to devices through which to learn were at significant risk of falling severely behind in their schooling (Turner, Pothong and Livingstone 2022). Similarly, there is a recognised digital divide when it comes to online research: how do you engage with an entire population when there is unequal access to sufficient Internet connectivity to perform an interview online? Ramsetty and Adams (2020) also highlight that those voices that become invisible in such a situation are going to be the most vulnerable, and potentially the most important for careful consideration in any situation. Running in person gameplay sessions was the closest that could be possible, in this situation, to try to address this potential inequality. In at least one case, one of the families that participated in the gameplay sessions in person referenced a lack of consistent Wi-Fi access, impacting schooling, during the period of lockdown: this is a family that would not have been reached during the online interview period. That said, even offering reimbursement for travel to in-person sessions was problematic for a number of potential families: due to the process required by the University for refunding travel expenses, the families would have to bear the costs until the reimbursement would be processed — a process of at least two weeks. The time taken to travel and return was also problematic. Several families outside of the immediate location of the in-person gameplay sessions (London and Canterbury) could not afford to bear the financial and time costs. In contrast, the online gameplaying sessions reached families in the North East and West of England, Scotland, Northern Ireland, and Wales, and could be scheduled in one-hour or 90-minute sessions that were convenient for them. Unlike other researchers have found (Pocock, Smith and Wiles 2021), the dropout rate for online sessions was not poorer than for in person sessions, with almost all arranged sessions being attended as agreed, without need to prompt or rearrange.

That is not to say that the online sessions were entirely without disadvantage. Pocock, Smith and Wiles (2021) list a number of potential disadvantages to online qualitative work, including higher dropout rates (as discussed above), and reduced control over technical issues occurring at the participant's end. In practice, neither of these issues were problematic, with no interviews or gameplaying sessions having to be abandoned due to technical issues. Pocock also noted that it could be harder to select and recruit participants online: this did not pose that much of a problem for this research, as a result of having a large potential participant pool from the Prolific survey respondents; each family that participated was also asked if they knew of anyone else who would be willing to participate. The logistical issues of evidencing informed consent, as discussed in Pothong and Livingstone (2022a), required a little consideration: getting consent forms returned online was a little harder than in person — but not much, as either participants were happy to take a photo of the signed consent form and email it back, or reply to the email containing the consent form confirming that they had consented.

Finally, the amount of time we spent at home was instrumental in considering undertaking the autoethnographical diary study discussed in Chapter 5.3. Such reflexive work, rooted in family life, would have felt much less useful in the time before the pandemic, where each family member, no matter how young, spent significant hours of their day outside of the home. This societal shift — which may last, to certain degrees, beyond the period of pandemic — helps to underpin the importance of getting security about home IoT devices right, as the home becomes a hub for significantly more activity, both personal and professional, than before.

3.9 Chapter summary

In this chapter, the thesis methodology was outlined at a high level, justifying the choice of various research methods, and explaining the process behind the analysis undertaken. Furthermore, the impact of the COVID-19 pandemic on research was considered, in particular the pros and cons of the need to perform significant amounts of research online. Further details on the specific methods implemented in each piece of research are incorporated into the chapters on the research themselves; and with this understanding, the next chapter, Chapter 4, outlines the first piece of research carried out, that of interviews and a survey of families in relation to their use of home IoT devices and understanding of cyber security.

Chapter 4

Discussing and managing cyber security of home IoT devices

4.1 Introduction

The literature review undertaken in Chapter 2 underlines the fact that little prior work appears to have been done to understand the adoption of home IoT devices affects both adult and child family members, taking into account differences between individual interaction preferences and abilities, what data the device may collect and level of awareness about how to use such devices securely. In recent years, sociotechnical research on issues of privacy and security of home IoT devices has focused almost exclusively on the privacy aspect, in particular, understanding of users about the collection of data. Other cyber security issues have not been considered so widely in this context.

There has not been targeted academic research based upon those devices that are most commonly used in a typical home, much less how families might use such devices or discuss the threats and risks that accompany their use. It was felt that such fundamental questions should be asked of participating families in the UK to address RQ1: What is the level of awareness exhibited by interviewed and surveyed families in the UK in relation to the cyber security of home IoT devices that they own and use?

Asking such questions would allow for an initial understanding of the participant families' (as a proxy for families in the UK) knowledge about appropriate

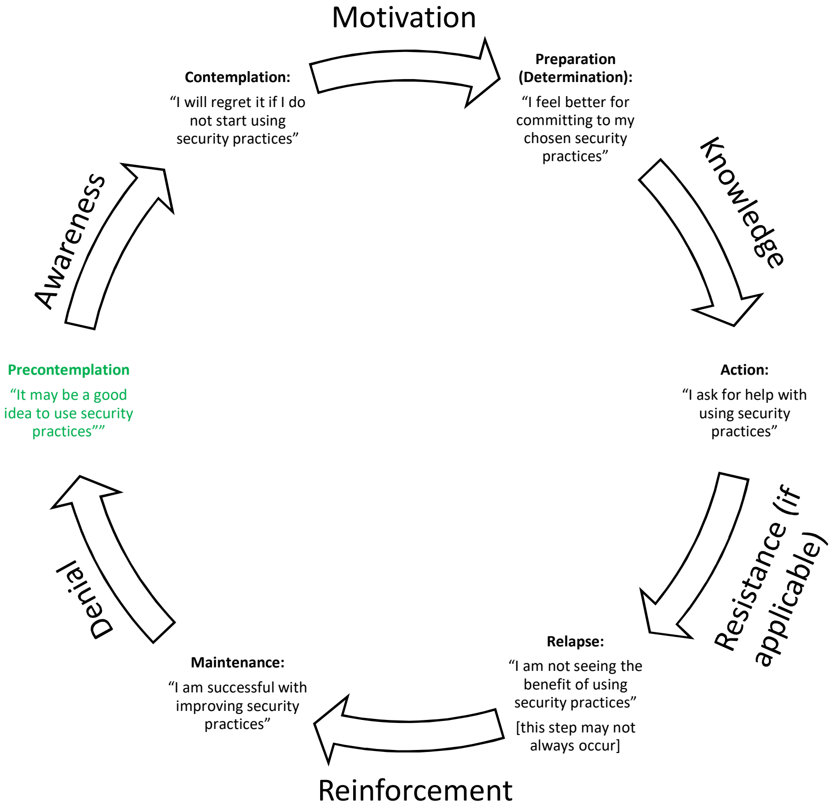

Motivation
Preparation (Determination):
"I feel better for committing to my chosen security practices"
Knowledge
Action:
"I ask for help with using security practices"
Resistance (if applicable)
Relapse:
"I am not seeing the benefit of using security practices"
[this step may not always occur]
Reinforcement
Maintenance:
"I am successful with improving security practices"
Denial
Precontemplation
"It may be a good idea to use security practices""
Awareness
Contemplation:
"I will regret it if I do not start using security practices"

Figure 3: The precontemplation stage of TTM, as adapted from Faklaris, Dabbish and Hong (2018)

types of cyber security measures and measures to use in conjunction with their home IoT devices: namely, the level of awareness that they exhibited about the topic, and where the majority of participants were in the TTM cycle (as discussed in Chapter 1). It was assumed that the participants involved in this research would be in the very first stage of the cycle, precontemplation (as shown in Figure 3). Was this an accurate assumption? This knowledge would then serve as a basis for understanding the starting point for further education and training opportunities presented in this thesis: what was already known, and what would need to be introduced, and built upon, to improve awareness in relation to appropriate cyber security for home IoT devices?

It was considered that a survey would be beneficial in providing breadth of answers – that is, it would be able to target a wide number of participants, who could help to determine the prevalence of home IoT devices and some level of understanding as to who manages the devices and how. Furthermore, the opportunity was taken to ask further questions about the knowledge of cyber security of adults and children at home, whether they were aware of cyber security in the news and what the adult who completed the survey believed their children were learning about cyber security at school. The set of questions used can be found in Appendix A. This survey will be referred to as "Survey 1".

During preparation for the work undertaken in Chapter 6, the opportunity arose to conduct a second survey to understand if the answers to some of the fundamental questions posed in Survey 1 were also relevant in 2022. It was considered reasonable to perform this check again for some of the key questions posed in Survey 1, given the rapid rate of change in the use of digital technology as a result of the changes in life caused by the pandemic between 2020-2022. The set of questions used for this survey can be found in the appendix J. This survey will be referred to as "Survey 2".

Semi-structured interviews with family units, that is, both adults and children, provide depth that complements the survey findings. In particular, interviews allow for time for discussion and reflection on use and levels of understanding in a way that the tick-box answers of a survey do not. They also, crucially for this work, allow for the voices of the entire family, and not just the survey taker, to be heard. The interview protocol can be found in Appendix B.

The interviews followed the survey, to dig deeper into questions around the family experience of home IoT device cyber security, giving the opportunity for both parents and children to discuss. As discussed in Chapter 3.3.1, the use of surveys and interviews allows additional levels of completeness and the ability to confirm the validity of responses and to give a sense of rigour to the findings.

4.2 Methods

In order to target the research, we broke the main RQ into two sub-RQs for analysis:

RQ1a: How do families explain and rationalise the cyber security related to their home IoT device use, and

RQ1b: How, and when, do families think about and educate themselves about home

IoT device security?

For both surveys and interviews, families had to be living in the UK with at least one IoT device at home. Survey participants had to be a parent or legal guardian of at least one school-aged child (between 4-18); for the interview, the participants had to be a family (of at least one adult and one school-aged child). The interview participants were recruited independently, and the agreeing adult was asked to complete the survey prior to the family interview, or by expression of interest after completing the survey. For a visual guide to the recruitment process, see Figure 4; this is explained in further detail in the sections that follow. Survey 1 and the interviewa received a favourable opinion from the University's ethics committee (CREAG) in July 2020; Survey 2 received a favourable opinion in December 2021.

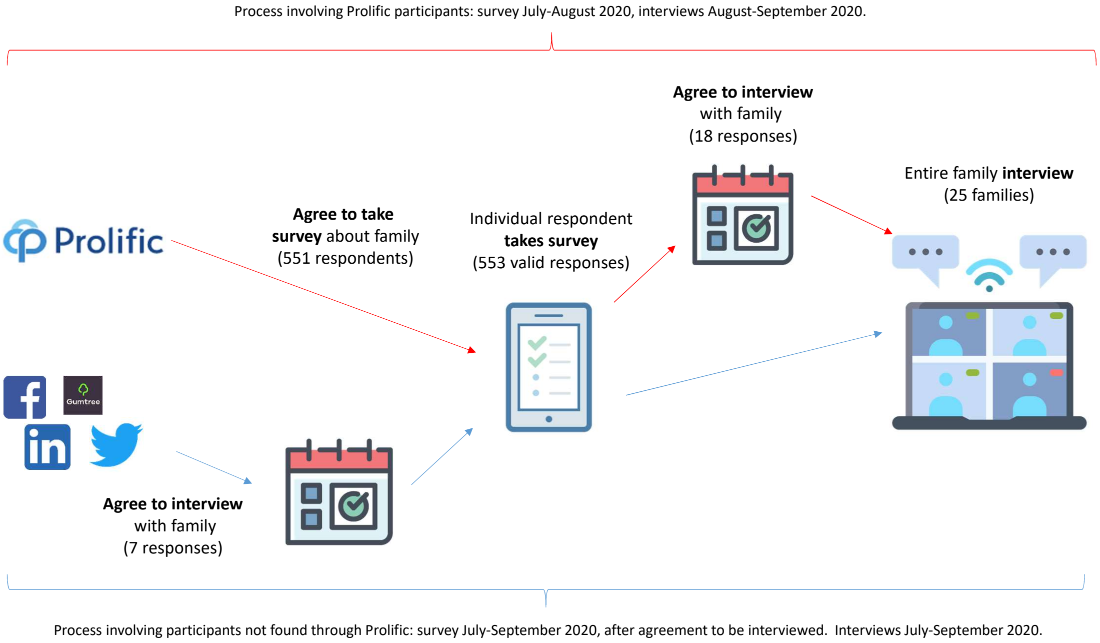

Process involving Prolific participants: survey July-August 2020, interviews August-September 2020.
Prolific
Agree to take survey about family (551 respondents)
Individual respondent takes survey (553 valid responses)
Agree to interview with family (18 responses)
Entire family interview (25 families)
Gumtree
Agree to interview with family (7 responses)
Process involving participants not found through Prolific: survey July-September 2020, after agreement to be interviewed. Interviews July-September 2020.

Figure 4: Recruitment process

4.2.1 Surveys

Survey 1 Design

The survey was designed to capture a broad range of information about the type of home IoT devices found in the homes of respondents, who bought, used, and managed them, as well as understanding the attention paid to cyber security in the home. Unlike the interviews, it was understood that only a single adult member of the family would be providing their interpretation of the family's use of such devices, giving the opportunity to ask specific questions (such as "Does one person take ownership of managing the device?") to understand the adult's role in family technology use. Each question gave multiple options for response, including a free text field for adding in options not covered.

The survey asked participants to list all their home devices, based on the list detailed in Chapter 1.1.1. Participants were able to add any devices they did not think were covered in the list. Then the participants were required to answer a range of questions about the one or two devices they used the most in the home. Participants were asked to focus on the most commonly used device(s) as a means of ensuring most, if not all, of the questions subsequently asked would have been considered at some point during ownership of the particular device(s). Questions were asked about devices that covered the entire use of the family, from the point of purchase onwards (e.g. "Was there a discussion about buying the device amongst household members (including children) before it was bought?", "Does everyone in the household use the device in the same way?", "Do you have to help the child(ren) in the house to use the device?"). These questions were asked to provide an understanding of how the participant perceived the role of home IoT device use at home, and where children in particular were involved in the decision-making and use of such devices, and can be found in Appendix A.

The remainder of questions about specific devices covered the understanding of cyber security and devices, broadly based on guidance provided by the UK's NCSC (National Cyber Security Centre, UK 2019). These questions asked about the setup of the device ("When the device was set up, were there detailed instructions?", and "Did the setup involve changing the password of the device?"), the current use of the device ("Do you know how you would completely delete the information that the device has collected?", and "Do you know how long or until when the software on the device is supported until?") as well as more general questions around device misuse and breaking ("Has your current device ever broken?", and "If the device broke tomorrow, what would your main concerns?") to assess cyber security risks against other risks that users perceived.

The final part of the survey asked for details of the experience of the participants with cyber security issues more directly: "Who or where do you turn to for support with digital technology issues?", followed by "Have you ever been a victim of cyber crime or data breach?". If they had, they were then asked if they had incurred a loss as a result of this (with loss intentionally not being defined as purely financial). Finally, they were asked if they were aware that the manufacturers of devices at home had reported a breach. In relation to cyber security and the family, they were then asked what aspects of cyber security they understood their children were taught at school and what they discussed at home, based on the list of topics covered in the English curriculum (Department for Education 2013), as discussed in Chapter 1.1. These questions aimed to reflect the awareness of the participant of his role as a potential victim of cyber crime and an educator about cyber security at home.

Survey 1 Participation

Both Survey 1 and 2 were hosted on Jisc's Online Surveys tool,[1] using the Prolific participant recruitment platform.[2] In total, 558 adults responded to Survey 1 during July and August 2020; 551 of them through Prolific and 7 from the interview recruitment process. Two participants were excluded because they only responded about a laptop computer and smartphone, not a home IoT device, leaving 556 responses for further evaluation. There were two attention checks in the survey: four participants failed both attention checks (0.72%); one of these participants was also interviewed. The three participants who did not pass the attention checks and were not interviewed were excluded from further review. The decision was taken to retain the person who was interviewed as it was possible to see the consistency in the responses between the interview and the survey. This left 553 valid responses for the final analysis. Survey participants recruited through Prolific were paid pro rata for their time, using the UK's Living Wage

[1] `https://www.onlinesurveys.ac.uk/`

[2] `https://www.prolific.co/`

Foundation calculated 2019/2020 rate of £9.30 per hour (Living Wage Foundation 2022) (with the majority of participants taking around 15 minutes to complete it). Those survey participants recruited outside of Prolific (as part of the interview process) were paid £5 in Amazon gift vouchers for completing the survey.

Survey 1 Demographic Information

The survey participants had a mean age of 42.32 years (SD 7.51), with an age range of 24-66. 138 (24.82%) were male, 417 (75.00%) female,[3] with one participant preferring not to answer this question. All participants lived in the UK at the time of taking the survey, with 473 living in England (85.07%), 41 in Scotland (7.37%), 21 in Wales (3.78%) and 18 in Northern Ireland (3.24%); although not intentionally sought, this proportion is broadly in line with the population breakdown across the countries in the UK as reported by the UK's Office of National Statistics for 2020 (Office for National Statistics 2021b). 81. 69% of the participants were employed full- or part-time, or due to start a job within the next month, with 2.51% considering themselves to be unemployed but job seeker. The respondents were asked to detail the age of their children. 17. 36% of the respondents (96) had a child 0-5 years old, 54. 07% (299) had a child aged 6-10, 53.52% (296) had an 11-15 year old, and 19.89% (110) had a 16-17 year old.

Survey 2 Design and Participation

Survey 2 was undertaken in April 2022. Participants were provided with the same list of devices as in 2020 (see Chapter 1.1.1, and asked to list the ones they owned. They were asked who took the responsibility for most decisions around device purchases. Participants were included in the survey if they were living in the UK, with children under 18 years of age who owned a smart TV, a smart home assistant or a streaming device. This is a different set of inclusion criteria from Survey 1, but the decision to limit participants to those who own at least one of the three device types came as a result of the predominance of those devices in Survey 1.

Other questions asked in Survey 2 looked to clarify the value of smart TVs, smart home assistants, and streaming devices as a tool for accessing the Internet.

[3] As found in other research on families, women tend to be over-represented in such results (Rode 2010).

This was used as a means of determining the amount of use smart features on these devices receive. We also asked participants in Survey 2 to rank the types of data that they thought were important to keep safe, who they thought was most likely to cause cyber security issues, and what would be the impact of having a cyber security incident with a device, based on predefined lists, with the option to add any that were considered missing in a free text field. Finally, we asked the participants what type of cyber security measures they used.

For detailed questions asked, see Appendix J.

Survey 2 had 792 respondents. A participant failed two attention checks within the survey and was removed from further review. This meant that the total number of participants in the survey was 791. As with Survey 1, the survey was hosted on Online Surveys, and participants were recruited through the Prolific platform. In line with the UK Living Wage Foundation's 2021/22 rate (Living Wage Foundation 2022), participants were paid pro rata for their time at £9.50 an hour.

2022 Demographic Information

In Survey 2, the participants had a mean age of 44.74 years (SD 11.32), with a reported age range of 20–84 —– six participants did not provide their age. 582 participants reported themselves to be female (73.6%); 204 male (25.8%), with five preferring not to answer this question. Differences in the data provided by Prolific between 2020 and 2022 mean that although all participants were included in this survey as a result of living in the UK, no further breakdowns of where the participants lived within the devolved nations were provided.

62.7% of the participants were employed full- or part-time. This is significantly lower than the ONS reported levels of employment at the same time (75.9% of the population having some form of paid employment (Office for National Statistics 2022a)).

73. 2% of the participants reported having two adults living in the household; only 10. 6% had only one adult living in the home, which is a lower proportion of single parents than reported in the UK (2021 figures showed 3m single parent families in the UK, representing 15. 4% of the families in the UK (Office for National Statistics 2022b)). There were 1214 children reported in total, equivalent to an average of 1.5 children per participant (with a median and mode of 1, SD of

0.72). The highest number of children reported to the home was six. A significant number of participants had a child under 1 year old at home (131, 10. 79% of all children). Other age groups were spread more evenly, roughly 5% each, with a higher peak of children aged 17+ (9.97%).

4.2.2 Interviews

Interview Design

The interview process was designed to build on the Survey 1 questions, by allowing the initial survey participants to expand upon their survey responses, and also to allow the entire family to add their views. The interview format was semi-structured, meaning that each individual could spend more time focussing on areas of concern (or awareness) for them; the interview protocol can be found in the Appendix B.

The interview process was designed in such a way that the researcher asked the children first, where possible, without interruption from their parents; the parents were then asked to answer the questions after the children had spoken. This allowed the parents to reflect on the children's answers, as in most cases, the parents had remained within earshot as their children were interviewed. The questions for the children were modified based on whether the child was in primary school (4–11 years) or secondary or tertiary education (12–18 years) in two ways: the expected level of knowledge was taken into account, based on the national curriculum for England laid out in (Department for Education 2013), but also the researcher modified the language used according to the age of the child. The questions focused on how each participant used the devices they chose to talk about: what device features did they like and dislike using, where they struggled to use the devices (and how they managed that). The participants were then asked, more specifically, about their understanding of what cyber security was. Children were asked to reflect on their understanding of what cyber security was, whether at school or elsewhere, and what they considered the biggest risks of using the Internet and home IoT devices were. Additionally, parents were asked to share any situations of being a victim of a cyber crime or incident, any times when they felt they needed to seek further information, and how they went about it.

Interview Participation

There were 25 interviews that took place between July and September 2020; the longest interview was 1 hour 15 minutes, with the shortest interview 20 minutes. There were 33 adults interviewed in total, 22 women (66. 67%), 11 men (33. 34%). There were 38 children interviewed, aged 4-16 (average age: 9.63 years, SD 3.59). Given the ongoing social distancing restrictions of COVID-19 at the time of the interview, three videoconferencing systems were used. Microsoft Teams, Zoom and Google Meet, based on the participants' preference. Where possible, all family members were asked to attend, in particular, to allow the researcher to ask questions of all family members and avoid the "driver" of device use answering all questions on behalf of less knowledgeable family members, and to understand the interaction the family had when discussing technology. This was not always possible, but for all interviews, at least one adult and one child from the family participated. Participants were sourced through posts on social media and message board sites (Facebook, LinkedIn, Twitter, and Gumtree), through expressing interest having completed the survey, and through the researcher's networks. The interview participants were rewarded with a £10 Amazon gift card if they were 18 years or older and a £5 Amazon gift card if they were under 18.

The details of the participants are in Table 5; throughout this chapter, adults will be referred to through the following coding system: A (for an adult), M or F (male or female), and their family's Interview Reference number, for example, the mother in interview 2 is called "AF2", the father in interview 3 is called "AM3". Children are referred to by C, their family's Interview Reference number, then distinguished by their age, e.g., the two children in interview 14 are referred to as "C14, aged 13" and "C14, aged 16".

How the children participated

The children interviewed had a wide range of ages, and so their participation and interaction in the interview process differed. All children reacted reasonably well to the use of videoconferencing and talking to the researcher; in two circumstances, the children asked not to be interviewed on camera, which posed no problems, as they were comfortable talking whilst off camera. In many cases, the opening questions, asking the children to describe the home IoT devices (more details

Table 5: Information of interview participants

Interview Reference	Number of adults	Number and ages of children
1	1	1 (15)
2	2	2 (12,15)
3	1	1 (5)
4	2	1 (4)
5	1	1 (10)
6	1	1 (6)
7	2	3 (7, 9, 11)
8	1	2 (5, 6)
9	2	2 (4, 8)
10	2	3 (7, 12, 13)
11	1	2 (7, 14)
12	1	1 (13)
13	1	1 (12)
14	2	2 (13, 16)
15	1	1 (7)
16	2	2 (7, 9)
17	1	1 (8)
18	1	1 (10)
19	1	1 (12)
20	2	2 (6, 9)
21	1	1 (9)
22	1	1 (8)
23	1	2 (14, 15)
24	1	1 (8)
25	1	1 (16)

on how this was handled by children of differing ages in the paragraphs below), followed by questions asking how they used them, were enough to allay any initial reticence to participate.

The youngest children (aged 4-5) did not sit by themselves to be interviewed: being interviewed in their own homes allowed them to wander around, and in certain circumstances, answer questions by doing — giving demonstrations of how they interacted with devices, rather than giving verbal explanations. Parents of children in this age group often re-framed questions posed by the researcher, not only to focus the child upon answering the question but also to use more familiar terms (for example, "how do you use the device?" was typically modified by parents in ways such as "how do you use Alexa?"). Parents of children in this age group supplemented answers with additional descriptions of device use and their experience of their children's level of understanding of how to use the devices. Children in this age group were able to think about and talk through how the devices they were familiar with might work, or make clear to the researcher that they did not know.

Children roughly between 6-10 would participate with a parent on- or off-screen. This provided the child with the assurance that it was safe and appropriate to answer the questions posed by the researcher (who was, of course, a stranger to them). In particular, children in this age group would not always give full answers to questions, so parents would prompt fuller explanations from their children when they recognised that this was needed. Children of this age did not seem particularly inhibited by their parents' presence, with at least one child quite happily discussing talking to strangers online, much to the shock of their parents, despite sitting right next to them. Children were able to think about how devices might work, apply concepts they had started to learn at school, and had some idea of risks that might come from the Internet, if not home IoT devices.

Children older than 10 or 11 years were able to have a conversation with the researcher by themselves, with little to no interaction with the parents while interviewed. In the case of children in this age group, many commented that they had become used to talking this way as a result of COVID-19 lockdowns and homeschooling in particular. Older children often also listened in to their parent(s)' responses, which sometimes promoted broader discussions between the parent(s) and the child(ren) about the question being asked.

The interviews were carried out by the researcher, recorded and transcribed. The transcripts from the interviews were subjected to inductive thematic analysis (Braun and Clarke 2006) by the researcher and a second researcher, as broadly described in Chapter 3.5.1. The researchers undertaking the coding performed the first round of coding entirely independently, starting with only the transcripts and inductively generating an initial set of codes. Once they had both finished this, they met to review similarities and differences in the generated codes. Discussions allowed for a consolidation and rationalisation of a joint code book — the inductive process meant that, in a number of instances, the coders had captured similar ideas with differently worded codes. After this discussion, both coders undertook a second round of coding to reflect the jointly created code book. Once this second round of coding had been performed, the codes were reviewed, and, at this point, a similarity test was performed using Cohen's *kappa*, giving a value of 0.63, indicating a substantial level of agreement. The agreed-upon codes, with description of primary sub-codes, can be found in Appendix C.

After the coding had been completed, the two coders initially independently reflected on the ways in which the codes could be classified into different themes, based on the overall idea or certain comments captured within a code. These tentative themes were then discussed by both coders together, as a way of determining areas of overlap and disagreement. These discussions, held over Microsoft Teams, allowed the researchers to screen share MaxQDA to help further discussions about the content captured in specific codes and individual quotes themselves. After these discussions, the researchers agreed on the themes discussed below.

4.3 Findings

4.3.1 Surveys

Survey 1

The participants reported having 2,326 devices in total: The top ten devices owned in general are reported in Table 6. There are three types of devices that appear to be much more prevalent than others: smart TVs, smart home assistants, and streaming devices (such as Google Chromecast devices and Amazon Fire TV Sticks), with 1,181 of these three devices being recorded.

The participants subsequently provided detailed information on 886 of these devices: the top 11 types of devices where the participants provided detailed information reported in Table 7.

Summary of findings: Survey 1

Table 6: Top ten reported device types (Survey 1)

Device type	Number owned	Percentage of all devices
Smart TV	437	18.57%
Smart speaker + home assistant	414	17.55%
Device connecting smartphone to TV (e.g., Chromecast)	330	14.02%
Smart meter	134	5.69%
Smart printer	130	5.52%
Connected children's toy	107	4.55%
Smart lighting	96	4.08%
Connected smoke detector	89	3.78%
Connected thermostat	84	3.57%
Connected doorbell	82	3.48%

This paragraph gives a high-level overview of Survey 1 findings presented below. Devices that are usually more expensive or integral to the household (e.g.,

Table 7: Top eleven devices: detailed participant response (Survey 1)

Device type	Number in depth questions answered about	Percentage
Smart TV	346	39.05%
Smart speaker + home assistant	207	23.36%
Device to connect smartphone to TV (e.g., Chromecast, Fire Stick)	106	11.96%
Connected doorbell	39	4.40%
Connected children's toy	33	3.72%
Smart meter	29	3.27%
Connected thermostat	18	2.03%
Smart printer	18	2.03%
Smart camera	16	1.81%
Connected smoke detector	13	1.47%
Smart lighting	13	1.47%

Smart TVs, refrigerators) were reported to be less new than other devices. The participants bought devices primarily after reading online customer reviews; Despite over half responding that they received detailed instructions, the majority of participants were unable to provide significant details about cyber security requirements, either at set-up or throughout the life of the device. The participants' primary concern about the device breaking was about the cost of replacement, not the implications for data security.

In general, the participants reported not helping the children in the household with the device or having concerns about children using the devices. This was especially the case for older participants or where there were older children in the family.

The participants overwhelmingly reported getting information on cyber security online; most of the participants were unaware of having been the victim of a data breach or cyber crime or if the manufacturers of any of the devices in their home had ever reported a breach. Reported learning at school and that discussed at home focused more upon online safety than cyber security steps: despite men being more likely to say they managed devices in the home, they were less likely to show knowledge of the children's school curriculum. Older participants appeared to be more likely to discuss cyber security strategies (rather than online safety) with their children.

Overall, these findings seem to back up the assumption that survey participants are at the precontemplation stage of TTM when it comes to the cyber security of home IoT devices (for a reminder of the cycle, see Figure 3. Some participants showed some awareness of more generic cyber security measures (such as the need for strong passwords on Internet-based accounts), but, of course, there was no way to determine how well these measures were implemented.

Quantitative Analysis

As a result of the largely categorical nature of the variables in the survey, in addition to descriptive statistics, the results were analysed using chi-squared independence tests (as described in Chapter 3.5.3)to determine any associations between three of the main demographic variables and different survey variables. The demographic variables considered were: the age of the participants (based on the age ranges of 30 and below, 31-40, 41-50, 51 and above) and the age of the oldest child (based on the age ranges of 0-5, 6-10, 11-15, 16-18) and the gender of the participant responding to the survey (male, female).

For the purposes of the chi-squared tests of independence, one record, of the one participant that answered "prefer not to say" in relation to their gender, was excluded as an outlier so as not to unduly influence the results. The sample size (N) used for calculation is different depending upon whether the question responded to was about a specific device, or about the participant and their family in general. For questions relating to the device, the sample size is the responses provided ($N = 884$); for questions relating to the participant and their family, the sample size is the number of participants ($N = 552$). The α value used throughout is < 0.05.

The following hypotheses were used:

The null hypothesis: There is no correlation between the particular demographic groups and how parents behave in relation to their discussions and actions around cyber security, in relation to their children and their use of IoT devices, represented through the variables of the survey question.

The alternative hypothesis: There is a correlation between the specific demographic variables and the compared survey variables when considering the discussions and actions around cyber security, between parents and children in relation to their use of IoT devices.

Those results that were statistically significant and where, therefore, we could reject the null hypothesis are detailed below.

Responses about devices

Age of devices Although there was a relatively even spread in the age of devices (0-6m: 18.40%, 6-12m: 24.94%, 1–2 years: 27.43%, 2+ years: 29.23%), it was notable that 139 of the Smart TVs (40.17% of the 346 smart TVs considered in the detailed questions) were recorded as being over 2 years old. Although with much smaller reported numbers, 100% of connected refrigerators/freezers (3 reported) and 55.56% of connected washing machines and tumble dryers were bought two years ago or earlier (5 of 9 reported). These larger devices, which cost more and are considered to be a standard fixture of a family home, are not only less new than many of the other devices in the survey, but were reported to be bought in spite of the smart/connected features frequently. Two of the three refrigerators / freezers were not purchased for smart features, along with 4 connected washing machines / tumble dryers and 66 (19.08%) of the smart TVs.

How devices were researched prior to purchase The respondents gave some insight into how they found reviews for the devices they were answering for. Participants either did not, or did not remember, researching 226 (25.51%) of the devices. Across the remaining devices, 572 (64. 56%) devices were purchased after reading "customer reviews on the Internet"; this option far outweighed more typically trustworthy means of establishing reviews, with only 116 devices (54 of which were smart TVs) bought after the participant read a review from a consumer protection body such as Which?, the UK consumer protection body.[4] Much more important seems to have been the cost of devices relative to alternative products (this being a consideration for 316 of the devices), as well as what the device looked like (a consideration for 226 of the devices), and whether the device was compatible with other devices in the home already (200 devices).

Who managed the devices? Devices reported on in the survey were typically managed by one individual, whether adult or child (633 devices; 71.44%). The decision for one person to manage these devices was reported as being intentional in 59.87% of the cases (for 379 of those 633 devices). There was a relatively equal split between whether people intentionally decided how their device would be managed, with participants confirming that there was no active decision-making process for management (or that they could not remember that this decision was made) for 428 of the devices (49.42%). Despite this, there were only 6 reported devices where the status quo had caused issues, ranging from disagreement over

[4] `https://www.which.co.uk/`

device use, to forgetting passwords (0.68%). There was a statistically significant relationship between sex and the reported management of the device[5] ($\chi^2(4, N = 884) = 57.21$, $p < .001$), with data showing that men were more likely to say they had sole ownership of the device management (62. 8% for men versus 39. 3% for women).

Security at the point of device setup The survey asked participants if they had received "detailed instructions" about how to set up their device. They responded that 536 of the 886 devices (60.50%) did have, with physically printed instructions included with 365 of the devices; 151 devices had prompts to visit a website, the remainder had a combination of both options. In one case, the instructions were also given by the retailer. The phrase "detailed instructions" was left deliberately vague for participants to interpret as they found appropriate. The survey showed that across all participants, an overwhelming majority of users did not know when their devices were supported until — this was not known for 843 (95.15%). Having "detailed instructions" made little difference to this figure: of the 536 with such instructions, participants reported not knowing the supported life of 505 (94.22%) of them.

Most of the users did not remember the setup that involved a password change: 495 devices (55.87%) did not require a password change, and the respondents did not remember for 196 of them (22.12%). Other activities that are related to the security and privacy of the device are also poorly understood by users: respondents did not know how to delete personal data from 685 devices (77.31%). There was a statistically significant relationship between gender and whether the participant knew how to delete personal data from the device or not ($\chi^2(1, N = 884) = 7.97$, $p < .005$); men were more likely to report understanding how to delete data from the device (29.6% for men; 20.4% of women). When asked to give their concerns should the device break tomorrow, participants were overwhelmingly concerned about replacing the device (67.16% of all devices), not over whether the data they had provided would become inaccessible to them (12. 87% of all devices) or subsequently deletable (0.23%, just 2, of all devices).

[5] With the options for management of the device being managed by: "me" (the participant), "another adult", "a child", "no one person in the household" or "a landlord".

Family Use

The respondents were asked about the type of help they provided their children to use for each device about which they answered the questions. For 687 of the devices (77. 54%), the respondents suggested that they did not feel the need to help their children. When they did give help, parents reported explaining how to interact with the device the most (93 devices, 10.50%); in the case of 83 devices (9.37%), respondents suggested that they managed their children's usage to avoid physical damage, or damage to the service the device provided. Respondents felt that they had no concerns about their children using the devices for 572 (64.56%) of those devices surveyed, and indeed, children were reported as using 682 of the devices (76.98%) by themselves, with very few reported issues.

Older participants provide less help and have fewer concerns The age of participants was shown to be statistically significant in terms of both helping children with devices[6] ($\chi^2(12, N = 884) = 67.18$, $p < .001$), and being concerned that children in the home may damage the device[7] ($\chi^2(6, N = 884) = 31.21$, $p < .001$). In particular, the amount of help given to children seems to decrease as the age of the parent increases, and the same is true of the concern around breaking the device. For further details, see Table 8.

Table 8: Age ranges of adult participants and interactions with their child(ren) (percentage based on all responses to the question by age range) (Survey 1)

Age range of participant	Children do not get help with devices	Percentage	I am not concerned about children breaking the device	Percentage	Children learn about cyber security topics that could be applied to devices at school	Percentage	I talk to children about cyber security topics that could be applied to devices at home	Percentage
30 and under	28	52.8%	26	49.1%	5	20.8%	14	58.3%
31-40	264	75.0%	199	58.5%	68	30.2%	125	55.6%
41-50	302	79.3%	256	67.2%	113	47.1%	165	68.8%
51 and over	92	92.0%	82	82.0%	42	65.6%	49	76.6%

The presence of older children makes for less help or concern for all children Similarly, the age of the oldest child in the family seems to make a difference to how the participant reported the help they provided or concerns they had for all of their children. When chi-square tests of association were

[6] With the options for "who helps the children in the home" being "all/most of the adults in the home", "another adult in the home", "no one in the home", "just me in the home", or "I don't know" (where 'me' and 'I' refer to the participant).

[7] With the options being "I have concerns", "I do not have concerns", or "the children do not use this device".

applied to the eldest child a participant reported as having, there were statistically significant outcomes as to the generally reported levels of help given to children ($\chi^2(12, N = 884) = 65.37$, $p < .001$), and concerns about breaking or damaging devices ($\chi^2(6, N = 884) = 36.36$, $p < .010$), as well as whether the participant believed their children were competent with the device or not ($\chi^2(3, N = 884) = 16.77$, $p < .001$). Survey participants with children in the oldest age range (16-17) were less likely, based upon the responses in the survey, to report giving help to any children in the family, or having any concerns about the children damaging the device. Interestingly, only when the oldest child was 5 or under was there a clear difference in the likelihood that the participants considered the children competent with the device. See Table 9 for more details.

Table 9: Age of oldest child and perceived ability (percentage based on all responses to the question by age range of oldest child) (Survey 1)

Age of oldest child	Not concerned about breaking device	Percentage	No help given with device	Percentage	Is competent with the device	Percentage
Between 0-5	19	36.5%	22	55.8%	28	53.8%
5-10	157	56.7%	183	66.1%	217	78.3%
11-15	251	66.8%	313	83.2%	297	79.0%
16-17	136	75.1%	161	89.0%	140	77.3%

Cyber Security in the Home

Where do users get support? There was a wide spread of answers to the multiple response question "Who or where do you turn to for support with digital technology use". 406 respondents (73.29% of the total number of respondents) said that they would turn to the Internet for support, with 217 respondents (39.17%) saying that they would also turn to other adults within the household. 64 respondents (11.55%) suggested that they needed no support, with similar numbers turning to friends (73, 13.18%), family outside the household (65, 11.73%) or children within the home (72, 13.00%). Very few respondents said that they made use of paid support (6, 1.08%).

Cyber crime and its effects The vast majority of participants had not, or did not believe that they had been, the victim of a cyber crime at any point (457, 82.50%). Of those that responded that they had, 26 reported having suffered a financial loss as a result. 65% said they had not, with 6 saying that they were not sure. 503 respondents (90.79%) said that they were unaware of manufacturers of devices that they owned ever having reported a security breach.

How is cyber security discussed at school and home? The survey also looked at the parents' understanding of what children learned at school about cyber security and Internet safety. The most common themes were "cyber bullying" (411, 74.19%), "stranger danger" (396 respondents, 71.48%) and "harmful online content" (390, 70.40%). More traditional cyber security themes were much less frequently recorded, e.g., "use of strong unique passwords" by 194 (35.02%) and "malware" by 107 respondents (19.31%). 87 respondents (15.70%) said that they were unaware of what their children had learned at school. There was a statistical significance between the age of the participant and the knowledge of those types of themes associated with home IoT device use[8] ($\chi^2(6, N = 552) = 35.99$, $p < .001$) (see Table 8), and also the gender of participant and the knowledge of these themes ($\chi^2(2, N = 552) = 12.27$, $p < .002$). The data shows that the older a parent is, the more likely they would be to report such themes; women (44.6%) were more likely than men (31.7%) to do so, too.

Finally, the survey reviewed discussions held at home by families about cyber security, and the Internet. 481 respondents (86.82%) reported having discussed the importance of not talking to strangers online. Other topics were far less uniformly discussed. 245 (44.22%) had discussed "what data might identify or reveal about you", and 212 (38.27%) had discussed the use of strong and unique passwords. 27.98% of respondents (155) had had discussions about how to minimize the risks of becoming a victim of malware. There was a statistical significance between the age of participant and the likelihood to discuss topics such as passwords and malware, instead of topics more closely linked to safeguarding, such as stranger danger[9] ($\chi^2(6, N = 552) = 17.73, p < .007$). The older the age range of a participant is, the more likely they would be to report discussing those topics more closely aligned to cyber security aligned to home IoT device use — see Table 8.

[8] With the participant responses being gathered into topics that were home IoT device related (strong password use, data management practices, malware, cyber crime, personally identifiable data), those that are not home IoT device related (stranger danger, harmful online content, cyber bullying) and "I don't know".

[9] As with the school test described in the previous paragraph, the participant responses being gathered into topics that were home IoT device related, those that are not home IoT device related and "I don't know".

Table 10: Top ten reported device types (Survey 2)

Device Type	Number owned	Percentage of all devices
Smart TV	711	16.16%
Streaming device	591	13.43%
Smart home assistant	494	11.22%
Smart meter	296	6.73%
Connected thermostat	239	5.43%
Smart lighting	206	4.68%
Connected smoke detector	200	4.54%
Connected doorbell	193	4.39%
Smart plugs	169	3.84%
Connected washing machine/tumble dryer	168	3.82%

Survey 2

The questions that overlapped with Survey 1, relating to device use and management of devices in the home, were corroborated by Survey 2, so will be briefly discussed here. 4401 devices were reported upon in this survey. 99.9% of participants reported adults managing the technology in the home. Only one child, a 15-year-old, was reported as managing devices.

It must be borne in mind that Survey 2 had different inclusion criteria to Survey 1, requiring ownership of at least one of a smart TV, smart home assistant or streaming device. As such, the numbers relating to ownership of these devices are much higher than Survey 1, and cannot be directly compared because of the inclusion criteria, but it is interesting to note in general that the top three devices reported as being owned remained smart TV — 711 (17.19% of all devices), second streaming devices — 591 (13.43% of all devices) and third smart home assistants — 494 (11.22% of all devices), of a total of 4401 devices reported. That said, there were more devices where more than 20% of all participants recorded ownership, more than in 2020. 296 (37.42% of participants, 6.73% of all devices) of participants reported owning a smart meter;[10] 239 (30.21% of all participants) a connected thermostat; 206 (26.04%) smart lighting, 200 (25.28%) a connected smoke alarm; 193 (24.40%) a connected doorbell, smart plugs (21.37%) and connected washing machine/tumble dryers (21.24%). For the top ten reported device types in Survey 2, see Table 10.

When asked about how often participants accessed the Internet through their smart TVs, smart home assistants or streaming devices, 65.5% of respondents said

[10] It is worth recognising that smart meters are both free for install and encouraged by energy companies in the UK, which possibly explains the large adoption figures here

they accessed it daily through their smart TV, 56.5% daily through their smart home assistant and 39.6% accessing the Internet daily through streaming devices.

Participants were asked to rank certain factors associated with cyber security relative to each other. The responses are detailed in Table 11, showing the ranking based upon the median ranking of each option, along with the ranking based upon the number of votes each option received. The intention behind these questions was to understand whether there were any stand-out concerns, in terms of the potential concerns about the loss of particular types of personal data collected (see Table 11a), the type of risks posed to devices from people (see Table 11b), and the most worrying harm if the device was somehow misused (see Table 11c). In each case, the participants were given the opportunity to add an additional option, if they felt it had not been covered.

Across all the questions, there were specific options that were standout concerns for participants. People were extremely concerned about the loss of financial data and subsequent financial fraud, with all other types of data or other loss being far less concerning. Thoughts about other (known) people accessing data were less strong – participants were the most worried about malicious hackers.

The final question in Survey 2 asked participants to detail out the cyber security measures that they regularly used. The most popular cyber security measure used was changing default passwords to strong, secure passwords (61.19%), followed by updating software (60.05%). Twelve of the nineteen options had over 20% of participants agreeing that they did it, with 59 (7.46%) saying that they did not know and 2 (0.25%) saying that they did nothing. The results are shown in Table 12.

4.3.2 Interviews

Summary of findings

This paragraph gives a high-level overview of the interview findings presented below. Both parents and children talked about threats and risks in the language of online safety — stranger danger, cyber bullying and so on — and scams, without association to the home IoT devices that they were discussing. The ability of children to spend money through home IoT devices was recognised by both parents and children but was often not acted upon until the children had spent money

Table 11: Ranking of participant concerns (Survey 2)

(a) Lost personal data

Potential Lost Personal Data Type	Median value (out of 10)	Rating based on number of votes received
Account log in	3	2
Biometric data	3	4
Contact info	4	6
Demographic info	6	8
Financial info	1	1
Network info	7	9
Passwords	3	3
Personal info	4	5
Usage info	5	7

(b) People accessing device

Potential people concerned about	Median value (out of 10)	Rating based on number of votes received
Adults	8	9
Children	3	2
Government	6	5
Internet service provider (ISP)	6	6
Malicious external	2	1
Manufacturers	5	3
Myself	9	10
Other family	6	8
Other guests	5	4
Tradespeople	6	7

(c) Harms from data loss

Most concerning harm of data loss	Median (out of 13)	Rating based on number of votes received
Your company/school/organisation financial loss	9	11
Financial fraud	1	1
Inability to perform core tasks	6	4
Inability to solve the problem	8	9
Inability to use devices	7	6
Inability to use home network setup as intended	8	8
Loss of access to services	7	7
Other financial loss	7	5
Personal data leak	3	2
Personal data loss	5	3
Physical harm to device	10	12
Physical harm to others	10	13
Physical harm to people	8	10

Table 12: Reported cyber security measures (Survey 2)

Cyber security measure	Number of participants who reported doing this	Percentage
Change default passwords to strong, unique passwords	484	61.19%
Regularly update software	475	60.05%
Use antivirus software	378	47.79%
Performing factory reset when getting rid of your device	371	46.90%
Use two-factor authentication	331	41.85%
Discuss appropriate device use with other home users	313	39.57%
Back up important data	303	38.31%
Regularly delete usage history	275	34.77%
Save/store passwords (in device, in password manager, in offline/physical notebook)	221	27.94%
Limit privileges or change default permissions	212	26.80%
Not using unsupported devices	204	25.79%
Limit sensitive data stored in the cloud	189	23.89%
Limit sensitive data stored in the device/supporting apps	151	19.09%
Put a cover over cameras attached to devices	146	18.46%
Use a virtual private network (VPN)	119	15.04%
I don't know	59	7.46%
Disable UPnP and port forwarding on your router	30	3.79%
Using a guest network	21	2.65%
Nothing	2	0.25%

without permission. Other types of financial fraud were not taken particularly seriously by parents (and were not considered at all by children) as the mechanisms for reimbursement through UK financial institutions were considered to be robust. Data loss from IoT devices was not raised as a concern.

Much as with their description of risks and threats, families described discussing online safety issues, when asked about how cyber security was discussed at home. Evidence of robust cyber security knowledge was relatively limited among adults and children, and the application of that knowledge was even poorer. Much stronger concerns arose, from both parents and children, about other aspects of home IoT device use — not security or privacy, but the costs of the devices, the interoperability capabilities of the devices, and the necessity of careful use to extend out their useful life.

Again, these findings also confirm the assumption that interview participants are at the precontemplation stage of TTM when it comes to the cyber security of home IoT devices (for a reminder of the cycle, see Figure 3. It is clear from the interviews that awareness — as evidenced by discussion between parents and families — and even action was being taken in relation to online safety, with the tricky downside that online safety was more or less completely understood to be a core part of cyber security, which only makes the steps needed to get to positive action around home IoT devices harder to achieve.

What do families consider the threats and risks of home IoT device use to be?

Stranger danger, scams: the same threats as posed by using the Internet directly All interviewed families did not differentiate between the threats and risks that home IoT devices pose, compared to other digital technologies that allow you to browse the Internet, and connect to social media in particular. Participants, too, presented no understanding of specific threats based upon their personal situation, but rather focused on generic threats with no clearly defined adversary.

The most talked about threat was that of "stranger danger" and that of inappropriate online contact with strangers. This is less applicable to home IoT devices, which participants recognised ("*Well, you can't chat to anyone on the [Amazon Fire TV] stick.*" (C5, aged 10)). The second most commonly considered threat was that of financial loss, through falling victim to scams, e.g., "*... giving your password, your bank password, to someone, and they then transfer all your money out. That kind of thing, I suppose. I can't think what else they could do that would bother me that much, or as much as that*" (AF2). This was a risk that parents felt strongly, and children were much less cognisant of, with suggestion that this was because they were not individually capable of managing their own finances. Interestingly, children who had seen attempted scams were likely to recognise them as such precisely because they targeted accounts they were not old enough to have ("*...I've got, like, 10 [text messages] this week [telling me that] my PayPal account has been hacked...but I don't even have an account.*" (C13, aged 12)).

Some parents felt that they could rely upon being reimbursed, should financial fraud occur, which minimized the harm (" *... my PlayStation 4 account was hacked. And they spent a lot of money. I got it all back. It was fine.*" (AM9)); this was from an expectation that any form of fraud would be reversed, or at least properly investigated, by traditional financial services firms, such as banks and credit card companies (" *... [if] someone's in your bank account, you'd call your bank, and they'd resolve it*" (AM7)). A couple of adult participants had experience of fraud through less traditional financial services firms, such as PayPal:[11] "*I just*

[11] PayPal explicitly explains that, because of its choice of location and registration for UK business, "The nature and extent of consumer protections may differ from those for firms based in the UK." (PayPal (Europe) S.à r.l. et Cie, S.C.A. 2021)

noticed all this abnormal spending activity. PayPal weren't particularly interested, I have to say." (AF8). The participant here was not reimbursed.

Unauthorised spending on devices is not as concerning as fraud Unauthorised spending on devices did not appear to be considered "financial fraud" for our adult participants, despite being a much more possible threat of home IoT devices. Perhaps as a result of being interviewed during periods of COVID-19 lockdowns, limiting the number of people that could enter the home, any unauthorised spending was considered almost exclusively in terms of children in the home, and as such was considered to be a restriction that parents should manage, even if they were unaware of the ability to do so: "*Oh yes, ... you ended up spending £5 on some terrible game, because we hadn't yet realized we'd not blocked it ...*" (AF6). The prevailing feeling, even among the children who discussed it, was that children might be expected to spend money accidentally when using devices, without realising what they were doing ("*I've got a password for my profile...so I don't spend money by accident.*" C22, aged 8). Those with family accounts on shared devices described instances of receiving an email about online purchases made by the child's account, and having to have a discussion with the child after the event. Only in one instance did a parent give an example of making the child repay the cost of the downloaded goods — a significant sum was spent on video games, by chance in the run-up to the child's birthday, making paying the parent back with money received as gifts a straightforward event. Had it been any other time of the year, the child would not have had the money to repay the parent.

Data loss is not an active concern Participants did not exhibit particular concerns about the loss or theft or data of themselves or on behalf of their family from any devices (home IoT or otherwise), or even the ongoing use of personal data by devices and their manufacturers. Some adult participants were sanguine about data loss, e.g., by saying "*we all just live now assuming that our data has been stolen and [we are] waiting for something bad to happen*" (AM23). Children, too, exhibited signs that they were aware of the risks of making their personal data available to others, whether through accident or design. In answer to the question "what is the biggest risk of using home IoT devices?", some children responded as follows: "*Your information being shared and people knowing what you do on the*

Internet...because you could get hacked or something" (C10, aged 13); "*I think, just accidentally giving my information*" (C12, aged 13), "*Accidentally sharing information that is going to come back to you and put you at risk*" (C23, aged 15). Children interviewed under the age of 13 did not talk about data loss as a risk.

Two families with more hands-off devices, such as robot vacuum cleaners, smoke alarms or thermostats, seemed genuinely puzzled by the notion that they would discuss these devices with their children, or that there would be security implications. In both cases, the children were typically reported as being interested and disruptive with the devices for a period, then ignoring them. Upon pressing, one parent explained their thought process about the smart thermostat: "*I would teach them to use it in the same way I would teach them to use anything else ... as [child] gets older, I would like him to load the dishwasher ...*" (AF9). When the time came, they would be showing their children only how to use the manual overrides for the smart devices in the home, not expecting them to use apps, or have any more significant control over the management of the data. When asked about data collection from smart home devices, this family felt comfortable with their expected data use by the manufacturers: "*I know they collect all the information. I know they try and use it to make money.*" (AM9). Another participant, heavily bought into the Amazon ecosystem of home IoT devices, expressed frustration that the most effective way to limit data collection, or to opt out of data use for improvement, was to activate a setting that might see them not receive future features: "*I changed some settings in the app that stopped them because they can listen to your recordings... And you can turn off the ability for them to listen to it. It's like a weird setting because it comes up with an option that says you might not get any of the new features if you turn this off, and I'm like, 'I like new features!'*" (AM16).

Linking "hackers" to the Internet, not home IoT device use Some children considered "hacking" to be the biggest risk, but could not necessarily explain what hacking meant, who might hack or what "being hacked" might look like in anything more than vague terms, e.g., "*they can change your password, so you cannot log into anything*" (C24, aged 8) or "*to me hacking means all data is stolen then it is sold*" (C18, aged 10). Children also framed this data capture in terms of smartphone or social media use (“*... phones have, like, tracking information, so they know where you are*” (C13, aged 12)), rather than home IoT device use. Several parents were unsure whether younger children recognised that home IoT devices connected to the Internet in similar ways to computers or smartphones (“*They don't understand that Alexa is connected to the Internet.*” (AF20)). When asked, most children were confused by the question of how a home IoT device might work: “*[Alexa] is a program. So people put in questions and answers. So yeah, it's like Google.*” (C10, aged 12); “*It's a good question. I don't know. It's magic!*” (C23, aged 15). Children seem to have a level of knowledge about data collected when using the Internet directly, but are at risk of not making the link between personal data collection, potential misuse and home IoT devices.

Threats to the home No adult participants raised potential threats to the home from home IoT devices, whether in terms of facilitating burglary or other physical damage. Conversely, two sets of parents explained how their connected home surveillance systems had enabled assistance in arresting a burglar in their neighbourhood (“*We were able to send pictures to the police.*” (AF2)), and in feeling more secure after past events around the house (“*I think just having it there prevents things.*” (AF19)). Children seemed to be more aware of physical damage that might arise from devices, and considered these risks more urgently than risks to personal data in two cases: “*There are a lot of things plugged in down there — they could set fire!*” (C19, aged 12); “*I think the most dangerous thing is getting water inside it...that's the only thing that's dangerous about it.*” (C5, aged 10). These concerns were not shared by their parents.

Cyber security knowledge gathering, sharing and adherence within the family

Discussion as a family... The most common way that interviewed families reported themselves managing any type of cyber security was through discussing it as a family. Should a child want to use a new app or device, many families expressed a process of discussing guidelines — length of use at a time, who and how they could communicate with people, what they could download, for example. Despite bringing the topic up when asked about cyber security, families recalled talking more spontaneously about online safety issues that they saw arising from the Internet (posting inappropriate content, not talking to strangers) than more strictly cyber security issues. Whether explicitly understood by the parents or not, the importance of a trusting relationship for this type of discussion was clear: "*... we talk to them a lot, and tell them to tell us in any situation*" (AF7). Children often referred to asking or learning from parents when they were unsure ("*I just call Mum and Dad*" (C7, aged 7), "*I [watch] my parents do it*" (C11, aged 14)).

...but not about home IoT device security There were no reported instances of interviewed families discussing home IoT device security together. Some parents suggested that they might use items in the news as a means of having conversations about specific security topics with their children, although, when asked about what news stories they had seen recently that made them consider their own home IoT setup, no one interviewed pointed to a specific story about a home IoT device being compromised. Neither parents nor children could explain, when asked, in much detail, as to how the devices they used worked: "*I don't actually know — no one has ever asked me that question before.*" (C17, aged 8). Yet parents seemed to assume that at some point there would need to be a discussion, without taking steps to understand the technology further. As AF5 explained: "*What I'm guilty of is I don't really think about it in any depth. You know, and probably because my children are still fairly young that you don't sort of think any further than what you need to [do right now].*"

Some parents with a larger age gap between children reflected how they seemed to have missed having conversations with their older, teenage children, because advances in digital technologies had happened relatively recently. Conversely, their younger children seemed to have grown up with, and just "understood" core functionalities of devices in the home instinctively, expecting devices to have touch screens and to stream programs on demand, for example, without understanding the technologies behind the device: "*He knows what he's doing when he's looking at it, but ask him what he's done. He wouldn't be able to tell you.*" (AM24).

Children's awareness of cyber security All children recalled that they had had classes at school about certain aspects of computer use. Most talked of having annual reminders of "stranger danger" and "cyber bullying", and using programs such as *Scratch*[12] to learn programmatic thinking and the fundamentals of coding. Only one child actively discussed being taught about malware (C23, aged 14). No children reported being taught about IoT products at all, with one child commenting that "*It would be nice to know just how different technologies worked, not just spending all the time on computers*" (C2, aged 12). Many children found school's approach "*all common sense stuff*" (C7, aged 11), and "*just talk[ing] about the same thing every time*" (C5, aged 10).

Most children interviewed indicated that they knew something about strong passwords, but typically had one core password that they used ("*I have my passwords all the same, so I remember it! But if you hack one account, you hack all of them!*" (C13, aged 12)), varying them should they need to share details with others ("*... if my friend and I may want to make an account where we all have access, I will use a password that is not my original password.*" (C5, aged 10)). Beyond this, children exhibited little cyber security knowledge that could be considered specific to home IoT devices: one child had read an article about how to delete their search history from their smart home assistant: "*I think I probably just saw something about it like on social media: 'This is how you stop your Alexa from knowing all your secrets'.*" (C23, aged 14).

Seven families had instances where a child expressed knowing more than a parent about the Internet generally, or specific security features. In these instances, children pointed out gaps in their parents' knowledge, but gave no indication that they would be expected to teach or help their parents further. For example, C13 (aged 12) showed frustration that his mother "*didn't understand the safe tick*" that the antivirus software they used provided to show the safety of websites. AF13 followed this by saying "*you'll have to show me!*", suggesting that the willingness to learn may be present, but not necessarily obvious to the child. Despite the suggestion that children may be on a par with their parents, there was no instance where a family expected the child to have a part in the security or management of communal devices, even if the child had an interest or exhibited accurate knowledge about security.

Parents' awareness of cyber security Ten of the adults considered themselves to be quite confident in the security of their homes. Either they thought

[12] `https://scratch.mit.edu/`

themselves "*fairly savvy on things*" (AF1) or felt confident that devices come ready prepared to avoid any kind of security breach "*Well, I suppose a lot of the devices such as the Echos...those kinds of things that kind of come pre-set up to be defensive*" (AM2). AM16 was aware of the potential for insecure home IoT devices to be used as a means of getting access to an entire network, but put faith in well-known devices: "*I read something about someone who put a Wi-Fi kettle on their network, and then someone had hacked into it...and gained access to the whole [network]... It can be a bit dodgy, but I trust the Amazon system, the Alexas...*" Participants that were confident of their abilities to secure computers did not provide evidence of having more security measures set up for smart home devices (for example, discussing guest networks, non-standard router settings or additional home networking) than users who were not confident when asked. Almost all adult users, and some of the older children, suggested that, should they need to find information about any aspect of security, they would search online, and assess the responses based on their judgement or prior experiences: "*Slight cliché, but Google, Google, and then I look at what looks like a legitimate organisation. I don't have, like, a specific way in mind, but I think I'm able to tell based on, you know, how the website looks.*" (AF9).

When adults were asked how they would like to receive information about cyber security, answers ranged from getting it from trusted technology TV shows, popular UK consumer champions, private companies, or even school. There were some parents who thought that this might be the remit of the government, but were unclear where it might sit (Researcher:"*Which areas of the government?*" AF25: "*I would say, probably [the Department for] Education...*"), or if there was even sufficient budget for the government to do it usefully ("*...maybe the government, but I don't know how the government actually have the resources.*" (AF8)). AM3 reflected that it would be helpful if there was an "*NHS* (National Health Service) *for cyber security*". The UK'S NCSC, who run the national security awareness campaign CyberAware,[13] amongst other awareness campaigns, was not mentioned by any participants.

[13] `https://www.ncsc.gov.uk/cyberaware/`

Parents' cyber security application Several adult participants expressed their inability to understand what is needed to secure the home and act accordingly, relying on other adults in the home ("*My husband brings stuff in the house and I have no clue. I can't tell you exactly what we've got...I've got no clue how it works or anything about it.*" (AF2)), or not thinking about it ("*I'm one of those people who probably doesn't think about security. I just go along until the disaster strikes and then yeah, I mean, obviously, I've got you know, passwords for our various things, but I mean, I don't sort of you know, think about it in that much depth.*" (AF5). Three adult participants equated being secure with having antivirus software ("*Once I download it, I am happy for the year.*" (AF13)) — even when not being sure that it would carry over to the home IoT devices they had: "*...[using antivirus software] was just kind of what got drummed into us when we were younger and when we first had computers, but with all the other kind of connected items, you just assume it's...in there, I guess.*" (AF6). Other participants understood that antivirus was not the sole means of keeping their home secure, and was not on their home IoT devices: "*I have Norton on everything apart from the TV.*" (AF 17). This gap was noted as if the home IoT device did not require any additional protection. Some participants considered free antivirus to be superior to paid-for versions ("*...I found a lot of them, if you'd shop around, the free ones are just as safe as the subscription ones. I mean, I swear on AVG Free for most of it. I still swear with that over £60 Norton every time.*" (AM24)). Given the practice of selling the data of users of free antivirus software, this may, in fact, open the user up to different security issues (Soni 2020).

Where cyber security knowledge was lacking Only one interviewed adult participant used a password manager for themselves, with another participant writing passwords down in a notebook. Two other participants expressed awareness of password management software, but dismissed them as too complex and tricky, or incompatible with not having access to technology all the time (one participant, unable to use their smartphone at work, was unable to access their bank account because the details were stored in the password manager). Other adult participants did not consider password management outside of their own memory a necessary practice. Some were confident that they could store a range of passwords adequately without further assistance ("*I'm fairly on the ball myself with it, to be honest, so I don't ever see the need [for a password manager]*" (AM24)), many expressed some small discomfort, or guilt, at knowing that they did not follow guidance that they knew to be important ("*I have the same passwords pretty much. Just like, a couple of letters changed. I'm terrible, yeah I know...*" (AF21)). Those adults participants asked had not changed the password on their router ("*It's too bloody long!*" (AM7); "*...I just put that in the too boring/too hard basket.*" (AF1)), and retained the router given to them by their Internet Service Provider. Children did not reference using password management software themselves, or having any discussion with their families about how to manage passwords of home IoT devices, and the potential for misuse when a single account is tied to a communal device.

Few interview participants, and no children, reported using multifactor authentication (MFA). In the majority of cases where individuals did report using MFA, it was only done after being the victim of a cyber crime, resulting in fraudulent activity ("*[the experience] made me go and turn on [MFA]*" (AM9)). MFA is, of course, less obviously used in home IoT devices directly, however equivalent steps, such as requiring a PIN for purchases through an account linked to a home IoT device, were typically not activated by participants. As with password management, there was no report of discussions within the family about the use and benefits of MFA.

Most adult participants were not completely sure as to whether their devices received automatic software updates, or whether they needed to be involved in the process. There were no participants who were aware of how long they expected their devices to be supported for, with some participants misunderstanding the question ("*[supported life] is probably similar to a normal energy bulb*" (AF16)). This is quite striking compared to Survey 2's outcome, where 60.05% of participants stated that they regularly updated software. Software updating was not discussed between families as a necessary process. Three children mentioned the importance of automatic software updates — but only one in relation to a device other than their smartphone (an Amazon Fire TV Stick). Six adult participants talked of their assumption that updates were automatically done, and took little time to consider it: "*when they get notifications they'll do it, but it's not a conscious thing.*" (AF14, about the children in the house). Both adults and children expressed a desire to manage their device updates, either because they did not want to have their use interfered with at the moment ("*I feel like it's an informed choice when I do things*" (AF2)) or because "*I feel like it slows the phone down*" (C25, aged 16).

Other home IoT concerns: costs, interoperability A much larger concern than security, particularly for those with a larger number of home IoT devices, was how to expand their smart home within their budget, and keep devices functional for as long as possible. Some participants were proud that they had been careful with old smart home assistants that were still functioning: "*...none of [my Echos] have ever broken. Some of them I've had since right at the beginning.*" (AF19). One participant with a significant smart home set up recalled that, with individual devices being so expensive, building up a smart home system was a slow process involving second-hand devices and constant interoperability issues. Older devices that this family had did not have full functionality, compared to newer devices, suggesting being out of supported life. Another family, unaware of the security implications, talked at length about how these interoperability issues made life a little more frustrating and a little less smart than they would have liked ("*Having to have a bridge like that is really annoying...why does Phillips [manufacturer of smart bulbs] need a bridge [to work with other home IoT devices] when none of the others do?*" (AF19)).

There were agreed-upon strategies to ensure that children took care of their devices — some children recognised that a device broken by them would not be immediately replaced ("*I don't want my [device] to break, because I won't be getting another one!*" (C6, aged 6)), where other families employed strategies such as this: "*We make them spend their own money on stuff like that. Hopefully promote a sense of like, you know, 'I bought this, it's mine, and it's my responsibility.'* " (AF7). Younger children in particular exhibited signs of friendship and care towards smart home assistants ("*[C4. aged 4] considers the Google Home part of the family...they have conversations in a very friendly way.*" (AM4)), or seeing them as integral ("*just part of our house*" (AM16)).

4.4 Discussion

The survey and interviews described above aimed to provide answers to RQ1: What is the level of awareness exhibited by interviewed and surveyed families in the UK in relation to the cyber security of home IoT devices that they own and use?. When entering this piece of research, the researcher had made the assumption that participants would not be further through the cycle of TTM than precontemplation, the very first step (see Figure 3). Some participants' families showed evidence of being further around the cycle when thinking about cyber security and online safety as it pertains to the Internet on a computer: not necessarily useful or transferable to home IoT devices. Considering the placement of participants around the TTM cycle is extremely helpful in defining the remaining pieces of research, in terms of exploring how to understand the levels of training and education that could be needed to build a level of awareness raising. As a start, the participants were clear that they would primarily go online to find information should they need it. Does the information available online provide adequate training to support positive action? And why is there a complete lack of awareness in relation to the way that home IoT devices might need cyber security? Are there specific factors that might need to be considered?

In terms of the RQ, there were a number of specific findings (Research Findings or "*RFs*") that explain aspects of the answer and outline the next stages of research. These are explored below.

RF 1: Families are happy to use devices, particularly smart TVs and smart home assistants, but do not consider security

The interviews and the surveys showed that families were happy to use and integrate home IoT devices in their homes, and did not take particular steps to inform themselves as to how to make these devices more secure. The most common devices were smart TVs, smart home assistants and streaming devices by quite some margin in both surveys;[14] both devices that are designed to collect significant amounts of users, and can be used for entertainment purposes by all members of the family, young and old. The adults and children interviewed had

[14] With the caveat, as mentioned earlier, that the inclusion criteria required respondents to own at least one of these three devices.

some level of understanding of how having home IoT devices increased the collection of personal data, and that misuse of such data by someone with malicious intent could be bad.

The interviews and surveys indicated several reasons for the lack of knowledge and subsequent action by participants. As indicated by Survey 1's results, people did not notice news stories about their devices, and may miss stories of data leaks and other breaches, thus not taking actions when needed. The interviews highlighted how adults and older children were resigned to data being taken and occasionally leaked; the survey results suggest that people are often unaware of, or immediately unaffected by, any breach. Regardless of their feelings about this, if individuals want to use such devices, they have to accept the terms of use, which often requires full data collection to be turned on for complete device functionality. Furthermore, cutting corners with, or not using, cyber security measures rarely causes directly applicable, irreversible harms, which reduces the incentive to try to change.

Both the interview and Survey 1 participants also made it clear that the Internet was the core means of security support. Rather than having a proactive security stance, the interviews in particular painted a picture of turning to the Internet for reactive guidance once something had gone wrong, rather than turning to friends, family or even the manufacturer or professionals.

RF 2: **Families do not have a clear understanding of the threats and risks their devices may pose**

The underlying concerns of parents in particular, around stranger danger and financial fraud, suggest that they did not recognise the difference in threats and risks posed by home IoT devices, compared to using the Internet on a home computer. Children echoed this, speaking almost exclusively of threats posed to them on social media, and risks typically stemming from "hackers", external to the family. This focus on external "hackers" was backed up in Survey 2 results, where they were the most feared in terms of illegitimate access to the participant's data by quite some way.

Survey 1 showed a complex relationship between the age of the participant and their actions in relation to their children — regardless of the child's age: although, the older the parent, the more likely they were to report talking to their children about cyber security measures that could be applied to home IoT devices, they were much less likely to offer their children support with such devices. This shift perhaps reflects the adoption of digital technologies over time — younger parents, more likely to have experience of digital technologies as ubiquitous and for interacting with others, seem to focus more on the use of the devices, with older participants being more concerned about security, a finding echoed elsewhere (Help Net Security 2022).

There is the overwhelming feeling that threats posed by home IoT devices are too impersonal and too remote for many people to feel compelled to take interest. It has long been considered that individuals do not find themselves interesting enough — or not wealthy or valuable enough — to be hacked (Howe et al. 2012) and in this light, it is understandable that the families interviewed spent more time discussing the much more manageable and realistic risks of talking to strangers and over-sharing personal data online.

It also does not help that stories, such as the home network being hacked through an insecure smart kettle, as mentioned by one of the interviewees, have a faintly ridiculous edge that undercuts the severity of having a home network compromised. Conversely, other potential threats that can arise from a malicious party accessing the types of data that can emanate from a smart home can be extremely distressing to consider, given the potential for harm to property and person, and how little the user might be able to do to protect the household. The 2019 incident of an individual hacking into a Ring camera in a child's bedroom and pretending to be Santa, talking directly to the children (Noor 2019), is one such upsetting example. Not only is this reported to be an attack widely possible due to software especially designed and distributed for the purpose (Cox and Cole 2019), but Amazon, the owner of the Ring device family, has repeatedly refused to acknowledge their responsibility for the harm and distressed caused, blaming users' insecure practices for facilitating the hacking (Paul 2020).

The psychological harms of an event like this need to be appropriately considered when considering threats, particularly when taking decisions for, and discussing alongside children or other dependents. Agrafiotis et al. (2018) considered the range of potential psychological harms that may occur to victims of a cyber breach — ranging from embarrassment and discomfort, to shame, depression and guilt, over an extended time period. Within a family setting, these types of feelings can be difficult to discuss, or may affect different family members in different ways. The importance of effective cyber security measures — strong and unique passwords, and regularly updated software in particular — is even more important when manufacturers may cite a user's lack of management of the security features to avoid liability.

RF 3: There is a lack of opportunities for learning for both adults and children

Both the survey and the interviews show the lack of appropriate education opportunities for both adults and children around cyber security. Children are more easily approached in school settings, but the status quo in the curricula applicable in the United Kingdom is not teaching appropriate security for home IoT devices or capturing the interest of children. Those children interviewed found cyber education at school repetitive, learning little that they did not already know about some topics (notably the safeguarding aspects of Internet use), and little to nothing about security topics. This confirms the findings of Pencheva, Hallett and Rashid (2020), focusing on cyber security at school, found that students generally are very tech-savvy, but treat online safety and cyber security as the same subject. The survey, furthermore, showed how important it is to ensure all children in a family receive the same education in a school setting, as it appears to be the case that the presence of older children in a home setting reduces the amount of attention given by parents to ensuring careful home IoT device use and secure cyber security measures of all the children.

Education for adults, outside of formalised education, in this space is extremely difficult to land effectively (Bada, Sasse and Nurse 2015), and the efficacy of such education depends upon personal and social norms, in many respects. Our interviews did not get as far as asking what types of message would be personally effective for participants, given the basic lack of knowledge as to how the devices worked on the part of the participants. However, participants did give a suggestion of the types of organisations and groups that they would like to hear from. These ranged from the government and related bodies, to trusted people with influence (such as particular TV shows and consumer champions) or manufacturers. The reliance on turning to the Internet for advice shows a lack of knowledge that could possibly be bolstered by these channels. Of course, this depends on how well trusted organisations are, which is a factor that will change from country to country, as will the societal approach to parenting, and managing personal risks. As an example, Kritzinger, Bada and Nurse (2017) found that, in comparing cyber security message approaches between the UK and South Africa, the UK's messaging focused upon the responsibility of the individual to protect themselves, rather than being a communal effort. This ties in with the argument in Renaud et al. (2018) that cyber security in the UK is becoming "responsibilized", with individuals expected to manage their own risks. This is not a particularly unusual expectation, also seen in the USA (Haney, Acar and Furman 2021), but, as the interviews showed, if individuals have inaccurate understandings of where they are protected, and what the actual threats and risks are, it is extremely unlikely that they will manage these risks effectively.

RF 4: **Parents promote careful use of devices, the importance of saving money and using consumer protection frameworks — but not security**

Children interviewed did not report witnessing active risk management from their parents. Survey 1's results showed the extent to which users did not know the details of their devices' security features. The interviews showed that families did not routinely talk about cyber security strategies that home IoT devices may need to use, such as the deploying of password management strategies, using MFA or the importance of regular software updates. This finding seems a little at variants with Survey 2, where participants reported relatively high levels of, in particular, software updates (60.05%), MFA (41.85%), discussion at home (39.57%) or password management strategies (27.94%), which may indicate a number of things:for instance, participants may have become more aware in the two years since the interviews, or that there might be an overestimation of the participant's use of some strategies in theory against practice (as seen both in the interviews here, but also in Chapter 6). Additionally, women were less likely to manage the devices in the home, or report understanding how to use them, but take more ownership of understanding what their children learn at school, meaning that the parent that may be less capable or confident is the one overseeing the children's education in relation to applicable cyber security. This finding may need to be approached with caution, however: other research has found that gender is not a statistically significant indicator when it comes to the ability to use cyber security measures and skills (Branley-Bell et al. 2022). What is found, however, is that men are more likely to self-report higher levels of self-efficacy; that is to say, men report themselves as being more confident in their abilities, but this confidence is not necessarily proven out when tested.

Parents promoted ideas of relying upon recognised consumer protection regulation, particularly in the case of fraud, but also in ignoring children who believed electrical safety could be an issue. Adults in the UK are accustomed to a rigorous consumer standards framework, with the ability to approach financial services firms for reimbursement where there is fraud without "gross negligence" (Financial Ombudsman 2021), and levels of assurance around electrical safety.[15] The interviews show that, for example, adults in the UK are used to being protected by strong consumer protection measures that should cover most cases of fraud — but crucially, not "gross negligence" when, despite being the victims of fraud, they were deemed not to have taken the proper precautions (Brignall 2020). Although adult interview participants were extremely concerned about financial fraud, a finding corroborated by Survey 2, few had enabled settings to limit purchases on applicable home IoT devices, and no family considered the ease with which significant sums of money could be spent fraudulently, potentially without recourse.

Families also modelled behaviour about extending device life through careful use. In a family context, this poses the problem that devices are not necessarily as secure as people might expect, leaving them open to attack in ways that may not be covered by consumer protection regulation, yet remain damaging to those affected. Instead, children are taught the importance of managing the cost of device use from their parents. Parents may look to second-hand devices to reduce the cost of expanding their smart homes, agree with their children that they must take care of those devices that they use, and use free security software. There is the common practice of applications being free at point of use, typically making the developers money through selling data collected on the users, which can be extremely invasive when a software is designed to control an entire system, as is the case with antivirus applications (Soni 2020; Ekambaranathan, Zhao and Van Kleek 2021). However, normalising the downloading of free software may

[15] Such standards include the Kitemark (`https://www.bsigroup.com/en-GB/kitemark/`) and the CE mark (`https://www.gov.uk/guidance/ce-marking`).

increase the chance of downloading a malicious app (Vass 2020); although directly a concern on smartphones, similar threats from careless downloading of skills (the smart home assistant applications equivalent of apps on mobile devices) have been shown to exist (Lentzsch et al. 2021).

4.5 Conclusion

The findings from the interviews and surveys present an underwhelming and complex answer to *RQ1*. Families, on the whole, do not discuss and manage cyber security proactively, rather assuming that disaster will not occur, or that if it does, it is the work of hackers who, most likely, would penetrate the network/device regardless, and that a mixture of consumer protection and reactive information finding will suffice when bad things happen. They certainly do not actively discuss, or have opportunities to learn about, cyber security as it pertains to home IoT devices in the same way that they might discuss aspects of online safety, meaning that children are learning the importance of careful device use to save money, but not to keep them secure.

These findings are useful to consider how to tackle the second and third RQs: "what knowledge is available online to those who wish to implement cyber security measures for home IoT devices?" and "How can the researcher effectively understand the awareness and motivation to consider the cyber security of home IoT devices shown by families?". *RF 1* shows that security is not top of mind when a device is brought to the house, reflecting that users may not be further than the precontemplation stage of TTM when it comes to cyber security measures for the IoT at home (Figure 3). This is helpful in terms of understanding how to frame the subsequent pieces of research, and how training, education and awareness raising must be sensitively considered: can existing methods help, and why might they not land well? *RF2* shows that users are happy to be reactive when it comes to solving problems, specifically by searching for answers online, the quality of which is not necessarily well understood. All four *RFs* point to device use that is not fully aligned with the threats and risks that are posed.

Chapter 5 takes these two strands forward, detailing the research done to understand what is available to users when they search online, and the practical difficulties that families have in considering, discussing and managing cyber security within their own homes, and the implications that those who have it can have when trying to mitigate the problems that inevitably arise.

Chapter 5

Issues arising when managing cyber security of home IoT devices

5.1 Introduction

This chapter turns to RQs 2 and 3: how can the researcher effectively understand the awareness and motivation to consider the cyber security of home IoT devices shown by families, and what knowledge is available online to those who wish to implement cyber security measures for home IoT devices? These questions help to explore how it may be possible to use existing information – or not – and explore whether there are gaps that may need to be considered to help more families move around the TTM cycle, since the previous piece of research underlined the fact that most families were still at the first, precontemplative stage (Figure 3). We will look at two pieces of research carried out separately to tackle different aspects of this question.

The first piece of research described in this chapter aims to better understand the issue raised in interviews and the detailed survey in Chapter 4 that although families were happy to adopt the use of devices, it is not likely to have a clear picture of the threats or risks that such devices pose. This leads to reactive management of issues when they arise, in particular, turning to the Internet for solutions. This first piece of research, therefore, explores how effective this solution is, by performing a content analysis of the information available online for home IoT devices, with additional emphasis on those devices that were most commonly reported as being owned in the survey and interviews: smart TVs, smart home assistants and streaming devices, such as Google Chromecasts and Amazon Fire Sticks. It was decided to use this type of research method because of the overwhelming response in Chapter 4 that questions and solutions would be "Googled". Understanding the likely efficacy of this process is extremely important when exploring the gaps that might exist. Exploring these gaps can help to support the types of knowledge-building and motivation development needed to find and maintain the use of relevant cyber security practises related to home IoT devices.

The second piece of research uses an autoethnographic diary study to analyse the author's own experience. This analysis can be used as a gauge to determine not only the reasons why families may not discuss or consider management of cyber security a high priority, but also as a way of determining how best to approach the subsequent work of finding solutions and proposing interventions in a population with — as far as the surveys and interviews suggested — little interest in, or ease of understanding, cyber security as relevant for home IoT devices. This particular method was chosen to spend time reflecting on the knowledge gaps and the impact for motivation as a user, rather than with the objective lens of a researcher. Alternative avenues could have explored the security of device use with individual families, for example, in a cognitive walk-through exercise or using a usability study to understand how well families might be able to set up appropriate cyber security measures for a new device. These methods may have allowed for an objective understanding of the problems that families involved might face, but would not allow the researcher to engage in the same level of reflexivity about her assumptions when approaching the final piece of research with families, which felt extremely important given the lack of awareness displayed by interviewed and surveyed families in Chapter 4.

Both of these pieces of research help to explore the complexities of cyber security specifically with a focus on home IoT devices. As discussed in Chapter 4, cyber security is very easily considered in the general, not the specific: these two pieces of research look at cyber security advice and experiences generally and consider how they could then be applied specifically to home IoT devices.

This chapter will first report the cyber security information review. It will then move on to the autoethnographic diary study. In both cases, background literature, methods, findings and implications will be discussed, before summarising the ways that the research addressed *RQ2* and *RQ3* and the impact on approaching *RQ4*.

5.2 Cyber security information review

5.2.1 Introduction

RF 1 and *RF 2* show that security is not top-of-mind when a device is brought into the house, and that users are happy to be reactive when it comes to solving issues, specifically through searching for the answers online. The availability of good quality, consistent and actionable information is crucial for keeping users safe and confident in their device use.

Given the paucity of information provided with many devices at the time of purchase, as confirmed in Chapter 4.3.1, and the likelihood of users to turn to the Internet for guidance, this section reports upon a critical study of the type of advice that home IoT device users might be presented with on the Internet to inform their cyber security measures. This type of content analysis can be very helpful in understanding not only the sorts of information that is available, but also who publishes such information, how search terminology can shape the results, and the level of detail provided in these sources, as discussed in Chapter 3.5.2. The data collection and evaluation methods are based upon similar methodologies used for security and privacy information across all digital technologies, such as Redmiles et al. (2020), as well as the understandability of data breach notices (Zou et al. 2019) and privacy policies (Fabian, Ermakova and Lentz 2017; Turner et al. 2021).

To get to a point of understanding the issues, we focused upon three particular sub-RQs:

RQ2a: What information is made available about cyber security threats posed to individuals using home IoT devices?

RQ2b: What information is given around how to mitigate those threats?

RQ2c: What type of organisations or entities provide that information?

This research built upon the findings of prior research. Tabassum, Kosinski and Lipford (2019) found that some home IoT device owners applied security knowledge learned from other contexts (such as from using computers and the Internet) when securing their home devices, despite the differences in threats posed and potential mitigating actions required. Even if individuals do act to implement cyber security measures at home, they could be overwhelmed with the number of actions that are deemed to be essential: Redmiles et al. (2020) found 374 pieces of actionable advice in reviewing publicly available documentation, and argued that what is needed is effective prioritisation of that advice. Prior to purchase, users rarely look for security and privacy information, but note that it is impossible to find if they do (Emami-Naeini et al. (2019a)). Recent research has used similar practices in relation to posted user reviews (Oygür, Epstein and Chen 2020) to understand what type of information users may encounter online on specific topics.

5.2.2 Methods

In order to understand what a home IoT device user might encounter when searching for information about how to secure devices that they may have, the decision was taken to search the Internet for cyber security guidance. This was done both in relation to general devices, using general search terms and reviewing the results that mentioned home IoT devices specifically, as well as for the most popular devices in the UK: smart TVs (and streaming devices), and smart home assistants, as found both in reviews such as techUK and GfK (2022), but also in the 2020 and 2022 surveys detailed out in Chapter 4.

The search criteria were generated in part through a word frequency analysis of academic articles (Ignatow and Mihalcea 2017), alongside some predetermined search terms, based upon the area of research (for example "how to secure my devices"). It was decided to undertake a word frequency analysis in order to ensure that no specific terms in relation to cyber security knowledge were missed.

To perform this analysis, the term "cyber security awareness" was entered into the Web of Science database (this database was chosen because of its broad coverage of academic articles), and the top 50 articles (ordered by date, most recent first) were downloaded and entered into the qualitative research software MaxQDA, where a word frequency analysis returned the top 100 words (of five letters or more) within these papers. These words were then sense checked, by searching for "cyber security + returned word" within Google and reviewing the first two pages of results to determine whether the search term produced results that focused on the provision of information about cyber security to users of home IoT and other devices. For details of the papers used for the word frequency analysis, and the top 100 returned words, see Appendix D. During this preliminary review, it was also determined that using the word "cybersecurity" as opposed to "cyber security" resulted in no difference of search results; as such, it was decided to use only "cyber security" when searching. It was felt that a general use of the term "cyber security" would be sufficient for this search, as a widely used and common term amongst users and manufacturers, given the focus on returning information as the user would find it.

Table 13: Generalised search queries

Search terms	
Cyber security information	Cyber security charities
Cyber security awareness	Internet of Things cyber security help
Cyber security knowledge	Cyber security help
Cyber security education	Cyber security support
Cyber security learning	Smart devices cyber security help
Cyber security training	How to stop being hacked
Cyber security organisations	How to secure my devices

The final list of generalised search terms are found in Table 13. Using these general search terms, pages in the results that had references to home IoT devices were captured for analysis. Search terms relating to specific devices took the form "How to secure my smart TV/streaming device/smart home assistant" along with "[manufacturer name] [device name] security" (e.g., "Amazon Echo security"). Specific brands were chosen based upon lists of "top devices for 2020" focused on UK consumers.[1] Having logged out of all browser accounts, cleared user history and using a VPN connection to a different IP address in the UK, the

[1] https://www.techradar.com/uk/news/best-smart-speakers, https://www.techradar.com/uk/news/best-tv, https://www.techadvisor.co.uk/test-centre/digital-home/best-media-streaming-box-3580569/

search terms were entered into three search engines: Google, Bing and Duck Duck Go,[2] and non-paid search results from the first two pages of each search query were captured, on the understanding that less than one in ten users are likely to go to the second page of search results (Ray 2019). The pages were retrieved between August and December 2020. For both results from the generalised search and specific device searches, each page was then reviewed, and those that had content referring to home IoT devices were then taken forward for analysis. In line with the recommendations in Kim and Kuljis (2010), in order to avoid problems of replicability arising from the ephemerality of website content, pages were printed to PDF. The printed versions of the pages were then subjected to deductive thematic analysis. The following codes were used, to collect information on including who produced the information and when, the type of devices considered, and the threats and advice given (in line with the methodology used in Blythe, Johnson and Manning (2020) and Turner et al. (2021)):

- The institution and industry of the producer
- The date of publication (where noted)
- The country of the producer
- The intended audience of the site (those that were discovered to have a professional or industry focus alone were removed from the list)
- Whether the producer was selling a product (including product sponsorship)
- The digital technologies mentioned
- The threats (and specificity of the threats) mentioned
- The cyber security advice (and the specificity of the advice) given
- Any links or references to other organisations

[2] These account for nearly 97% of all UK search engine traffic as of July 2020 (Johnson 2020).

5.2.3 Findings

Sources of information

The prominence of news and opinion outlets was clear in the results. 125 sources (53.41%) of the 234 organisations with web pages considered in the review were either recognised news organisations (such as The Guardian, Wired, CNet) or websites offering news and opinion pieces of varying levels of speciality and expertise, ranging from personal blogs to user-facing technology sites (such as PC Mag, ZD Net). The search also returned a volunteer-run cyber security helpline,[3] offering help across a wide range of cyber security issues. We also found that the favourable rankings of more traditional news sites acted to suppress sources of advice and information about device security in favour of prior security and data breaches: notably, a 2014 breach relating to Philips' smart TV range still dominated the first two pages of results, even in Google's Featured Snippets,[4] despite the age of the story. Although the majority of individual web pages returned were dated 2019 and 2020 (228 web pages, 53.40%, of 427 total web pages), 91 were undated, and 2 websites (from a retailer, and an antivirus provider) had content dating from 2011 (from the date given in the body of the article).

Only nine information sources of the 234 organisations were affiliated with global governmental departments; there were three consumer protection bodies (such as Which?[5] and Consumer Reports[6]) and five additional not-for-profit or charitable bodies. Conversely, bodies that may have been trying to sell a service related to security were much more common: there were nine antivirus providers (such as Malwarebytes and Kaspersky), and firms offering cyber security services (such as BullGuard, Digital Guardian and Cytelligence) accounted for 21 pages. There were 13 forum sites, both third-party (Reddit, Stack Exchange) and manufacturer community pages. There were no sites from ISPs returned in the results.

Reported threats

Examples discussed in the text are detailed out in Table 15.

[3] https://www.thecyberhelpline.com

[4] For more on Google's Featured Snippets, see https://support.google.com/websearch/answer/9351707.

[5] https://www.which.co.uk/

[6] https://www.consumerreports.org/

Type of threat	Count
Unauthorised access	144
Malware	22
Data theft	13
Botnet	9
Ransomware	8

(a) Top five: threat types

Type of advice	Count
Strong password management	149
Limit data access	145
Better home network security	143
Turn off features/devices	117
Update software	113

(b) Top five: advice types

Table 14: Threat and advice types

Discussions about cyber security typically arise from the need to secure something from a specific and meaningful threat. In the review, 57 individual types of threats were raised; for the top five, see Table 14a. The full lists of all advice types, threats and organisations found can be seen in Appendix E. 144 websites referred to some form of unauthorised access to devices, most typically "hacking", without further explanation (Table 15, #1). 39 web pages focused on either how to manage after you have been hacked or avoiding being hacked, typically presenting reactive advice rather than explaining why it may be necessary to take proactive measures ahead of an event (Table 15, #2). Malware and ransomware were mentioned a total of 30 times, with theft of personal data being mentioned 13 times. Botnets were referenced nine times. It is noticeable how many types of threat were referenced only once or twice throughout the review. 26 types of threat came up only once (examples ranging from domestic abuse, to ghostware and hacktivism). Lack of personal knowledge was framed as a threat (rather than a potential vulnerability) in five instances (Table 15, #3). In some cases, the publication of specific academic or industry reports were reflected in the reporting of several news sources (Table 15, #4). In these cases, the threats reported upon are typically accompanied by the researchers' views on how to mitigate the risk, albeit at a high level, often without accompanying links to manufacturer guidance for specific devices.

Table 15: Examples of advice given (as referenced throughout text)

Reference	Source/date	Issue raised	Link (all last accessed 31 March 2021)
1	IoT for All (2020) (IoT blog)	Generic threat explanation:“...they leave us vulnerable to cyber crime... [IoT devices] are top targets for hackers.”	`https://www.iotforall.com/iot-cyber-security-2`
2	Lifewire (2019) (consumer technology blog)	Reactive security guidance — things to do after you have been “hacked”: “no matter how you were hacked, you’re feeling vulnerable.”	https://www.lifewire.com/securing-your-home -network-and-pc-after-a-hack-2487231
3	IoT Wiki (2019) (IoT enthusiast blog)	Lack of knowledge a threat: “many individual users...still lack information about the risk” ’	https://internetofthingswiki.com/biggest-security-issues-iot-devices-face/1344/
4	Tech Crunch (2019)	Report of FBI advice on smart TV security	https://techcrunch.com/2019/12/01/ fbi-smart-tv-security/
5	Now TV (undated) (streaming devices)	Password guidance:“DON’T use a word that’s found in the dictionary”	https://help.nowtv.com/article/tips-to-help-you-keep-your-account-secure
6	Comparitech (2020) (consumer technology blog)	Password guidance: “Make changing the router password part of your monthly routine”	https://www.comparitech.com/blog/information-security/secure-home-wireless-network/
7	CSO Online (2016) (technology risk news site)	Don’t use devices as intended: “Don’t connect your devices unless you need to... turn off UPnP...be wary of cloud services”	https://www.csoonline.com/article/3085607/8-tips-to-secure-those-iot-devices.html
8	Lifehacker (2018) (consumer blog)	Non-specific advice: “If you’re lucky, your router can broadcast a ‘guest network’...”	https://lifehacker.com/how-to-keep-your-friends -from-trolling-your-chromecast-1828805478
9	Cytelligence (undated) (cyber security service)	Non-specific advice: top ten list with no further details (e.g.“Stick with protected devices only...Disable unnecessary features...Secure your network fully”)	https://cytelligence.com/cyber-security-and-smart-devices/
10	Digital Trends (2021) (consumer technology blog)	How to secure your Alexa device (with 12 suggestions)	https://www.digitaltrends.com/home/how-to -secure-your-alexa-device/
11	Wired (2020) (technology magazine)	Guest networks: “grant your you guests access to a Wi-Fi connection without letting them get at the rest of your network — your Sonos speakers, the shared folders on your laptop...”	https://www.wired.com/story/secure-your-wi-fi-router/
12	Kaspersky (undated) (antivirus software)	Guest networks: “[set] up guest networks for your IoT home devices”	https://www.kaspersky.com/resource-center/ threats/how-safe-is-your-smart-home
13	How-To Geek (2020) (consumer technology blog)	Guest networks: “you would connect all your IoT devices... and actual guests to the guest network”	https://www.howtogeek.com/659084/ how-secure-is-your-home-wi-fi/
14	Google (undated) (Android devices)	How to log your child into their Android device	https://support.google.com/families/answer/ 7158477?hl=en
15	Help Cloud (undated) (consumer security service)	Buy a more secure router: “[invest] in a sound WiFi router”	https://www.helpcloud.com/blog/cybersecurity -experts-and-iot-smart-devices-and-smart-homes/
16	Ready.gov (undated) (US governmental resource)	Implication of need to buy more security: “[use] a password manager...use antivirus solutions...use a VPN...”	`https://www.ready.gov/cybersecurity`
17	PCWorld (2019) (technology news site)	Implication of need to buy more security: “Our favourite password manager is xxxx...you’ll need to pay an annual fee, but it’s worth it.”	https://www.pcworld.com/article/3332211/ secure-android-phone.html
18	Real Simple (2020) (consumer blog)	Buy reputable devices: “If you want to have IoT devices around...a wiser route is going to be by shopping in Apple or Google’s walled gardens...”	https://www.realsimple.com/work-life/ technology/safety-family/smart-home -cyber-security
19	Norton (undated) (antivirus software)	Choose based on privacy and data policies: “What are the privacy policies? Will the provider store your data or sell it to a third party? How are updates enabled?”	https://us.norton.com/internetsecurity-iot-smart -home-security-core.html
20	The Guardian (2020) (news site)	Coverage of Sonos’ decision to stop software updates for old devices	https://www.theguardian.com/technology/2020/ jan/23/sonos-to-deny-software-updates-to-owners -of-older-equipment
21	eBuyer (2018) (consumer technology blog)	Software updates:“You should always update your smart devices...as soon as it becomes available”	https://www.ebuyer.com/blog/2018/10/smart -devices-and-security/
22	National Cyber Security Centre (2019) (UK government body)	Wiping device of data: “you should first perform a factory reset.”	https://www.ncsc.gov.uk/guidance/smart-devices -in-the-home

Types of advice needed and provided

In total, there were 1,342 pieces of advice counted in the reviewed web pages, which, when coded for advice type provided, a total of 54 unique topics. The top five advice types are listed in Table 14b; these are explored more now.

There were 149 separate instances of recommended strong password management (11.10% of the total pieces of advice given), many of which gave advice contrary to the current guidance from the NCSC to use three random words to create a strong and unique password. For example, two manufacturers explicitly suggested that words found in the dictionary should not be used (Table 15, #5), and suggestions to change passwords frequently were also common (Table 15, #6).

Limiting the access services have to personal data was the second most frequent type of advice given in the reviewed web pages (145 instances; 10.80%), although precise guidance as to what this means for specific devices was not generally explained. Disabling some features (such as Universal Plug and Play) or turning off the device (or router, or Wi-Fi) altogether was the fourth most common (117; 8.71%). The trade-offs of doing these actions were, again, largely unexplored (Table 15, #7). Specificity of advice was a common problem — the heterogeneity of devices left some pages assuming that devices had particular functionality as the premise of their advice (Table 15, #8), or providing a list of things to do with no guidance at all (Table 15, #9). Other pages gave so much advice as to run the risk of seeming overwhelming (Table 15, #10).

There were 143 instances of advice around improving the strength of home networks. Advice around improving the strength of the user's home network is particularly difficult to follow, as the exact, typically relatively technical, steps vary upon the router in the house. In the general searches returned, there was no guidance about smart home security provided by ISPs. Without further searching in relation to the router owned by the individual, at first glance it is impossible for the reader to know which pieces of advice (such as "use a VPN" or "set up a guest network") would be feasible for their current router. Setting up a guest network, in particular, was recommended, but the specifics of doing so were varied: some pages suggested putting all the user's devices on one network and anyone external on the other (Table 15, #11); others suggested keeping home IoT devices on one network, and the users' other devices and guests on the second (Table 15, #12); and there was also suggestion to keep your personal non-IoT devices on one, and your home IoT devices and guests on the other (Table 15, #13).

When manufacturer's pages were returned in the reviewed web pages they were typically in a wiki-format, for a very specific topic — focusing upon how to change a specific setting rather than why you might do this — with minimal visual guidance: a checklist of steps to perform a specific activity on a specific device (Table 15, #14). In contrast, sites not affiliated with manufacturers offered more generic advice. Not only did they provide little specific device guidance or explanation as to what that would protect against, but they frequently suggested additional products that come at additional costs. Some are explicit: buying a more secure router (Table 15, #15), or, less clearly, products and services that can come with a cost, such as antivirus software, VPNs or password managers (Table 15, #16, #17). Other advice given includes to be choosy with home IoT device providers (even at a risk of becoming locked into a single provider) (Table 15, #18), and performing pre-purchase checks such as reading privacy and data sharing/selling policies (Table 15, #19).

There was a striking lack of information about end of life device management, with the exception of the negative press relating to Sonos' decision to stop supporting older models in early 2020 (Table 15, #20), and general advice to "update software" (but not explicitly to be aware of the end of the supported life of your device) (Table 15, #21). Only the NCSC discussed wiping a device at the point of reselling or throwing away (Table 15, #22).

5.2.4 Discussion

The cyber security information review described above aimed to provide some answers to the second research question of "how families discuss and manage cyber security and home IoT devices?". In particular, the findings show that even if individuals were at a stage of exploring knowledge gathering to move from the TTM stage of precontemplation, there is not sufficiently robust information available to support their movement around the cycle in a meaningful way. More accurate and targeted guidance would be needed to support movement around the TTM cycle. There were a number of specific RFs to take forward to the next stages of research.

RF 5: Users need to understand what is a threat to them specifically to apply any cyber security information they might find

Before being able to manage risks effectively, however, users need to have more meaningful guidance about the types of threats that their devices may pose, so that they can appropriately evaluate what risk management means to them. This is a complex area, given the potential for misuse, abuse, and power imbalances (Ehrenberg and Keinonen 2021). Different threats mean that some users may be best off following different advice for the same device, but without an ability to accurately assess the threats and risks that the device poses to them, users are likely to fall back to behaviours that have worked for them before, which may not be appropriate in this case (Tabassum, Kosinski and Lipford 2019).

Furthermore, without an understanding of what the threats to a family may be,[7] untargeted advice may end up being an unhelpful, ineffective or expensive option. Advice to choose devices based upon more agreeable privacy policies or calls to do research before purchase and buy “more secure devices” highlight a lack of congruence between the advice and real life. Privacy policies are notoriously hard to read and comprehend (Renaud and Shepherd 2018), and offer no ability for the user to negotiate the terms of their use. Calling upon users to research devices prior to purchase suggests that sufficient information is available to make a useful comparison of security features — not only is it hard to find this information, it may not be meaningful or useful when found (Emami-Naeini et al. 2019a). Additional suggestions to use more software — ideally, purchase software — is problematic: it introduces another barrier to effective cyber security for those who cannot afford it, and it is unclear how to apply such software across all devices in the home, if it is even possible to do so. The attrition rates for use of such software is likely to be high, particularly if its value in protecting devices is not visible or obvious (Dupuis et al. 2019).

RF 6: Information about device security likely needs wider context to be accurately applied

A significant proportion of the guidance discovered in the reviewed web pages was not actionable for home IoT devices without further understanding or learning by

[7] For the types of threat that could impact families, see Table 1

the reader. This, in part at least, comes from the over-generalised idea that the webpages held about cyber security measure: that advice can be about general topics, not the specific, because the specific may be impossible to write about when addressing a diverse audience. The heterogeneity of home IoT devices, and the situations in which they are used, means that there may be best practices that are specific to the device and its use. Different designs mean that users cannot guarantee that they will be able to follow steps to disable settings, for example, to adhere to best security practices, assuming the specific device they have has the functionality to allow the user to access and alter security settings. It could be inferred from this that users would struggle to find the specific information they might need to solve, or preempt, a home IoT device security question or problem.

Furthermore, the most appropriate point to modify security settings may be at the home network, and not device, level. Calls to alter router settings, for example, are assuming that users have the technical confidence, sufficient access to the controls within the home setting, and that their routers have the functionality to do so, none of which may be the case (Zeng, Mare and Roesner 2017).

RF 7: Hard to find credible guidance

Governmental and consumer awareness resources did appear, often low down in results. Despite their relative trustworthiness and validity as relevant and impartial cyber security information, such resources are often indistinguishable from other sources in search results. These other sources may have financial interests in the framing of their advice (such as antivirus providers), or the guidance may be from irrelevant or out of date sources. Users would benefit from higher placement in search results of official guidance from governmental agencies and manufacturers to try and provide up to date, specific information; inspiration could be taken from the work done to place prominent information from recognised expert bodies at the top of search results relating to COVID-19.

5.3 Autoethnographic Diary Study

5.3.1 Introduction

The interviews and survey findings showed that security is not only not particularly important to families when thinking about home IoT devices, it is also barely recognisable as a concern. Given the state of precontemplation, what gaps are there in the day-to-day use of devices that may stop or at least hinder the ability to learn about, or even consider using, home IoT device security? *RF 2* showed that families do not understand the threats and risks devices pose in their specific contexts, with questions of cyber security being framed as ones of online safety. Furthermore, *RF 4* highlights what parents in particular do find important: careful physical use of devices in order to avoid damage to avoid unnecessary loss of money. Careful use of devices will certainly ensure that the physical device lasts longer, but often at a cost of losing security as the device ages because of limited periods of software updates. The lack of education around this for both adults and children (*RF 3*) is therefore problematic: how do families ensure that they understand how the devices they use should be carefully and securely used, particularly given the difficulties of finding relevant information should it be needed (*RFs 5–7*)?

The next phase of research, the autoethnographic diary study, allowed for a period of reflection on the role of the researcher in trying to understand both where cyber security fits in and how, as a result, to produce meaningful solutions to these problems. As a member of a family of exactly the type being researched, it was considered useful, and perhaps even important, to take a reflexive view (Delamont 2009) on how much cyber security came up at all — and why it did, if it did. In particular, would looking critically at how much engagement an expert (the researcher) has with cyber security in her everyday life help understand what sort of interventions may need to be taken in order to appropriately engage with families to promote understanding of cyber security for home IoT devices? Could it help to create a sense of empathy surrounding the difficulties that non-expert users might have in navigating cyber security in their daily device use? And what does that mean for how devices are intended to be kept secure?

The term "autoethnographic diary study" is used here to describe a piece of first-person research exploring the topic in relation to the broader societal and cultural setting, but using the feedback-style recording method of a diary study with multiple participants. It builds upon two research methods: the diary study and autoethnography.

Diary studies have been described in Chapter 3.3.4: it is a method a commonly used method within the Human-Computer Interaction (HCI) and Computer-Supported Cooperative Work (CSCW) research communities. In recent years, diary studies have been used to understand how adolescents (children aged 13–17) and parents manage online harms (Wisniewski et al. 2016; McHugh et al. 2017; Agha et al. 2021), how new parents approach baby wearable technology (Wang et al. 2017), how children with autism spectrum disorder use mobile applications (Putnam and Mobasher 2020) and how social groups approach joint privacy and security use of shared applications and devices (Watson et al. 2020; Chalhoub et al. 2021). Garg and Sengupta (2019) used a diary study, capturing information from parents with children aged 4-17, on their smartphone and speaker use. Through the entries in the study, they found that there were differences in how families used, managed and limited technology use dependent upon their socio-economic and ethnic status.

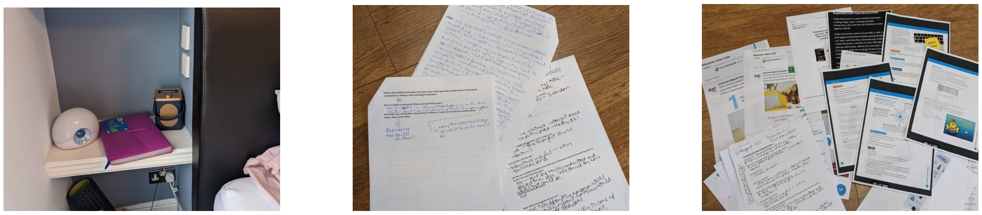
The diary studies mentioned above ranged in duration from two weeks to two months, allowing for significant data collection to occur from the participants, both in paper format and using online tools, with reminder capabilities built in. Watson et al. (2020) noted that the ability to track responses online was important, as they needed to chase a number of participants with phone calls to ensure they completed the diary. Hong et al. (2020) found that paper allowed for more flexibility in responses — although participants found managing paper diaries with digital artefacts hard to manage. Putnam and Mobasher (2020) found different problems with the diary study method: although the adult participants did not find the method of filling in the diary itself problematic, getting the children involved in the study to participate in a way that generated results to discuss in the diaries proved extremely hard.

Analysing personal use of devices can provide additional levels of empathy towards users and research participants to be taken forward in the design process (O'Kane, Rogers and Blandford 2014; Cunningham and Jones 2005); conversely, non-use of devices can also provide insights in that it allows for questioning and re-imagination of use (Lucero 2018). Reflecting on the use of closely related duoethnography as a research method, a 2019 paper highlights the importance of using personal experience to explore the "interactions between diverse users, devices and data" in intimate settings (Garcia and Cifor 2019); the family unit being one such example. This method could, in this case, help frame what interventions would be needed to get families to understand cyber security for home IoT (the fourth RQ), but only if the method of collating the diary works for the researcher first.

5.3.2 Methods

Following the receipt of a favourable opinion from the University's ethics committee CREAG in August 2020, the researcher undertook the research in her own home between 12 August and 31 October 2020. The study mostly focused upon interactions within the researcher's immediate family (two children, aged 6 and 3) and husband, although additional interactions with other family members (such as the researcher's parents and parents-in-law) that stayed in the home in this period were also captured when relevant. The additional levels of motivation around and knowledge of cyber security that both the researcher and also her husband, being a software engineer, had, was considered to be relevant, as subsequent analysis of the topics raised from the study could determine how many were raised precisely because of this additional sensitisation to the subject. Drawing upon the autoethnographic format, the researcher completed the diary entries alone, based upon her interactions and experiences with her family.

The diary study topic looked at how the cyber security of home IoT devices was managed and discussed between parents, children and any other relevant individuals within the home. Using a "feedback" style of diary (Carter and Mankoff 2005) in order to elicit broad responses to consider these answers, a set of daily diary prompts posed a series of open-ended questions intended for the researcher to reflect on the events of each day pertaining to home IoT device use and cyber security. The questions focused on what was said, done, and what emotions events raised, not dissimilar to the type of responses received in Wisniewski et al. (2016) (for example, "Was the conversation home IoT device use or cyber security related?" "Were there any subjects relating to devices or cyber security of those devices that you avoided talking about today? If so, why?"). The daily diary



(a) Bright folder kept by the bed to prompt daily reflection

(b) The pages of the diary prompts, incorporating free writing

(c) The full printed diary, with diary entries and printed artefacts

Figure 5: The diary study process and sample artefacts

prompts were printed and kept in a purple folder, along with pens and sufficient additional paper, next to the researcher's bed, in order to serve as a visual reminder to log instances at the end of each day (see Figure 5a). Entries were only to be recorded when there was something of relevance to be captured during the day. For the full list of prompts, see Appendix F.

The prompts did not change throughout the period, and daily reflections were collected primarily on paper, not electronically (see Figure 5b). This was for two reasons: the type of activities being considered were unlikely to be done routinely, meaning that using an electronic method for the purposes of eliciting immediate responses through reminders would not be beneficial; also, the use of paper allowed space for more reflection through unstructured feedback (Ayobi et al. 2018). The handwritten entries were typed up weekly. Any relevant information that was seen online (for example, social media posts) were treated as additional artefacts: they were collated and saved electronically, printed as necessary and analysed alongside the typed-up diary entries. In the end, the finished diary comprised of written entries, screenshots of social media, school curricula, scans of text books and e-mails, as well as a list of all home IoT devices (and those devices or digital technologies that interacted with the devices) (see Figure 5c).

Once collated, the complete diary was subjected to reflexive thematic analysis (Braun and Clarke 2006) by the researcher, as described in Chapter 3.5.1. Following McDonald, Schoenebeck and Forte (2019), it was determined that the analysis should only be performed by the researcher to preserve the personal and reflexive nature of the research.

5.3.3 Findings

How well did the autoethnographic aspect work?

An additional level of knowledge

Using the autoethnographic approach of having only the researcher record diary entries was important: in using the reflexive requirement of the study, would it be possible to further deconstruct the reasons why users may typically struggle with managing home IoT device cyber security? The additional level of knowledge held by the researcher about requirements and risks associated with device use was clear in a number of entries, giving an idea of privacy and security concerns that might not be considered by those without an interest. Sometimes the entries explored the difficulties of trying to set up devices in ways that are more privacy-preserving and allow for more controlled security: "*[The eReader] is defaulted to have Wi-Fi on all the time, with limited restrictions on access to the store. Switching off the Wi-Fi results in it warning you that it will cause problems...*" — diary entry, 15 October.

This instance also highlighted the difficulties of tailoring device use for children: the eReader was bought at a time of lockdown to help the researcher's elder child continue to read in a time when library access was impossible. There were a range of small barriers that meant the use of the device heavily curtailed and limited their privacy in a way physical books do not. To avoid the one-click purchasing of unsuitable books, the eReader's access to the Internet was limited, by tethering it to my smartphone. Children's library memberships could not be used through the library's app, meaning that my account (an adult account, with full access to all books) had to be used. Both instances required ongoing oversight for me, and a limitation of use for the child. As we came out of lockdowns, so the eReader was used less and less.

Other reported instances of acting out of a heightened interest in security were triggered by external events: for example, trying to find out more about a vulnerability, reported by a technology news site, in microchips used in her and her husband's smartphones:[8] "*We really felt that there was little we could do... we'd have to rely on our phone's manufacturer to manage the patching. It*

[8] `https://arstechnica.com/information-technology/2020/08/snapdragon-chip-flaws-put-1-billion-android-phones-at-risk-of-data-theft/`

unnerved us a bit, in thinking about it, that we found this in specialised press only — and certainly not in mainstream news sources. It's tricky having a little bit of knowledge: it often leaves you in a state of uncomfortable inaction...!" — diary entry, 18 August.

One further way in which additional levels of knowledge altered the family's activities was in the decision to spend money to purchase more secure tools. As discussed in Section 5.3.3, this also speaks to the resources available to the family, as where possible, paid for services for password management, antivirus software and VPN access, are used. During the period of the autoethnography, the researcher and her husband realised their smartphones were old enough that they could have reached the end of the period in which the manufacturer would support it with anything more than the most critical of updates. Confirming this was extremely challenging, as there was no official guidance from the manufacturer about how long they would support the devices. The clearest insight came from an Internet chat forum, where users had determined the likely supported life based upon things that the manufacturer had said in the past. That investigation determined that, indeed, our smartphones — despite working perfectly in every other way — should be replaced to avoid potential security issues, at a huge cost. This is an act that needs to be performed for every device in the home, and the risks of having partially supported, or not supported devices, weighed up in turn. Although, in the UK, legislation might make this easier in time (for example, the PSTI Act), it is still a large mindset shift to remember to review the details and replace a device that may otherwise be functioning well, rather than waiting for a device to fail obviously.

Where knowledge did not help

Having the written diary entry was helpful to contrast and explore the emotions felt when cyber security was working as expected — and when it was proving too complex. Negative sentiments were common throughout the diary, with words like "infuriating", "uncomfortable", "frustrated" and "frustrating" occurring three times each (in some 6,600 words of the full diary). Dealing with situations that were unresolvable, or that required significant time, knowledge and investment was hard — even when, as in the researcher's case, there was an interest in having the most appropriate security setup at home.

More positive words were less common — "amazing" occurred once, "benefit" and "excellent" twice each. Interestingly, these more positive records related to the potential use of devices, not aspects associated with security — there were, in fact, no records commenting that a device's security ostensibly worked. These entries, again, help to underline the types of experiences that stick in the mind when using devices as part of life: the researcher was inclined to think about security and go out of her way to apply techniques and settings that she knew of, and even then, security activities were framed negatively within the diary.

The diary entries recorded a number of instances where having cyber security knowledge did not actually help resolve the situation at hand. This was particularly the case when trying to help or communicate about cyber security issues with others. Trying to help a relative manage some unusual activity on a computer should have been an opportunity to help them walk through and improve their cyber security knowledge and use. Instead, the relative was so overwhelmed by the situation, and happy once their bank had confirmed no financial loss had occurred as a result of the activity, that they did not listen further. "*What struck us [researcher and her husband] was the complete lack of understanding, backed up with a defensiveness about cyber security practices...Almost everything we tried – both in terms of explanations of mitigating steps, and practically looking at and reviewing the devices – failed.*" — diary entry, 17 August.

The diary entries showed how having knowledge about how to make devices safe did not help when trying to explain why it was necessary to the children, even when they were keen to listen. The concepts were too hard and too abstract. For example, the children were particularly interested in the researcher's new smartphone: "*It was hard to find the words to explain why I had replaced it — I wanted them to understand that phones are only expected to have a life of around 3 years, but at the same time....they won't understand it! Not happy with the words that fell out of my mouth ('because...it could be dangerous.'). Not that they prodded further – they just loved that the cover wasn't black... They now don't care.*" — diary entry, 15 October. The smartphone had been replaced as it had reached the end of its supported life: without guaranteed software updates, it could pose a security risk. The complexity of these ideas, coupled with the uncertainty of the risk (it could pose a risk, should there be a particular set of circumstances), made it a conversation too difficult to have.

When the elder child asked what the router did, the best the researcher and her husband could do was say "*well, it's how the Internet comes into the house*", which "*felt useless even as we said it...*". Even if the words were there, the attention span of children for such discussions is extremely limited — the researcher concluded this entry in the diary with a feeling of relief at how quickly the child "*showed little interest...*" — diary entry, 12 September. One of the artefacts collected alongside the diary entries was the elder child's school curriculum for the year, which detailed the computing skills to be taught during the year. A combination of using a computer ("*how to use or navigate with a mouse*") and learning about "*the dangers that the Internet can portray*" made it clear how ubiquitous computing and the concepts associated with it are not something that the children can hope to learn about at school alongside encountering it at home.

The collection of artefacts included a number from organisations offering parents snippets of help for discussion privacy and being secure online with your children (typically as shown on social media websites like Twitter). The structure of organisations involved in "Internet safety" in the UK is vague and difficult to navigate, with a number of not-for-profit bodies and charities offering bits of advice, mainly on how to keep children safe on social media. Twitter campaigns from law enforcement agencies focused on the need to manage children's digital technology use within legal parameters, to avoid falling into cyber crime; other campaigns, from charities and not-for-profits, ran sponsored posts on Twitter that talk about "using privacy and security settings", with no further explanation as to what this meant in practice. Neither felt appropriate as a means of starting discussions with children who do not talk to people online, but do use devices ubiquitously daily.

How well did the feedback diary method work?

Frequency of reporting

The pilot diary study lasted 80 days, significantly longer than many documented diary studies, although shorter than many autoethnographic pieces of work. It generated 30 individual diary entries; in addition to the written diary there were 15 screenshots, two e-mails and the list of devices. Many of the diary entries were between 100–300 words in length, with the longest over 700. Despite placing the diary prompts in a convenient location for writing up, the researcher felt very aware of the number of days when there was little to nothing to report, based upon the prompts. Electronically saved information often had to be additionally printed to ensure that the thoughts about them were collected at the end of the day.

What was directly captured in the entries

The researcher found the feedback diary method, in particular with its open-ended questions, helpful as a means of being able to consider and reflect freely upon the situations arising during the diary period. The completed diary covered an extensive range of events, from buying new devices, to discussing reported security breaches and dealing with family device problems, to reflections upon the use of specific software on the researcher's smartphone.

Further analysis found that not all of the entries, however, directly contributed to the overall research questions. The entries and artefacts show that two types of cyber security arose in the diary: the "housework" of cyber security that is directly applicable within the home, typically relating to things like the device setup, and the "wider universe", reflecting interesting or concerning news stories about cyber security issues that cannot either be directly managed within the home, or that are not directly relevant. In particular, the diary entries allowed the quantification of the time spent considering each type: reading about the cyber security "wider universe" appeared in six entries; "housework" references to researching new devices prior to purchase, installation of those devices, and device management occurred four times in total.

Those entries that did reflect "housework" management of cyber security within the immediate family showed an important element: they were, typically, one-off events. For example, purchasing a new eReader for the researcher's eldest child allowed for discussion with the child about setting strong passwords, setting Wi-Fi access, and discussion about how and when books could be purchased or borrowed; this was recorded at the time of setup, and not subsequently.

Once set up in the home, however, questions of device security did not come up. Repeated use of devices seemed to breed familiarity and a level of comfort around its use. When devices were in situ and just functioned as needed, there was no further consideration about the invisible processes in the background that may need further consideration or management. Diary entries discuss long-used devices only in terms of the habitual nature of their use — both by parents and children, once the device was considered part of the family's setup. "*The kids are only used to streaming services, and so will often ask to watch programmes via the Chromecast, which allows for useful parental control of what they're watching (as we turn off autoplay). However, this also means that short programs...sees them asking for the next episode almost before the prior one has begun. This is tricky as it can see tired or impatient children grabbing the phone...*" — diary entry, 13 September.

The diaries also helped to reflect on the ability of children to consider security, and what that meant for discussions and learning opportunities. There were four detailed discussions about cyber security with the children — exclusively with the elder child. The younger child was captured in the diary as showing awareness of devices in the home,[9] but had no concept of the need for security. Some of these events allowed for moments of family discussion and collective reflection: for example, password use being mentioned in a television show allowed for a brief discussion of what a password is. In total, passwords were discussed with children three times and unauthorised purchasing once.

What was indirectly captured in the entries

The diary prompts did not have questions that required the researcher to consider aspects of her role and status, both within the domestic setting and also more broadly in terms of gender and economic status within society. Despite this, both aspects were strongly present within the diary entries, and add another level of nuance to be included in the analysis. Without a clear understanding of the space in which the researcher inhabits, it may be hard to understand where their experience differs from that of an average user.

Of particular note in this case was the economic status that the researcher's family has. The amount spent on new devices and security software in the period led to reflection upon how expensive maintaining appropriate device hygiene can be. The ability to replace those devices that are out of supported software life or use paid-for cyber security software such as password managers may well reflect best practice, but they are options that require sufficient disposable income to

[9] In particular the Google Chromecast that facilitated streaming TV shows.

make the decision to do so. For many, it could well be a poor decision — or an impossibility — to replace otherwise functional devices, or pay for cyber security services in a world where data breaches are common, but obviously tangible downsides are few.

5.3.4 Discussion

The autoethnographic diary method described above aimed to provide some more answers to the second research question of "how families discuss and manage cyber security and home IoT devices?". In particular, when looking at a family with higher than average levels of cyber security knowledge and, as a result, higher motivation to apply appropriate methods, the aim was to provide some information on how to produce interventions that might be meaningful to less engaged families. In particular, what barriers may need to be overcome to allow movement around the TTM cycle from precontemplation onwards? There were a number of specific RFs to take forward to the next stages of research, explaining the gaps that were explored.

RF 8: Cyber security rarely arises in everyday device use

The inability of the researcher to make daily diary entries felt like a concern, when analysis was performed. As recorded, in the 80 days of the study, the researcher produced 30 diary entries; a small number compared with similar studies with more participants such as Garg and Sengupta (2019), where the average participant entry rate over an eight-week period was 110, when asked to record information about all types of device use. Furthermore, only six of these entries captured active discussions with the immediate family about cyber security in the context of device use. However, in this respect, the autoethnographic diary method provides the person undertaking the study with a helpful guide as to when and how the topic fits into everyday life. If the individual performing the diary study, who has more interest and specific knowledge than an average user, reports infrequently, this in itself helps to get into the mindset of an average user and stops assuming a level of engagement that may not exist.

Deciding to use diary prompts requiring answers written on paper, rather than through an online system, facilitated what has been referred to as "writing as thinking" (Oatley and Djikic 2008). When there is something to report, having no limitations on the responses allows for a more reflexive experience, a process referred to as "critical subjectivity" in Garcia and Cifor (2019), even if some of the entries end up being outside of the topic of interest at the point of analysis. In particular, when considering a concept that is not widely understood by an average user — such as cyber security — the process of writing about instances of dealing with the concept as a more informed researcher helps to understand whether it is reasonable for an average user to consider it too. The majority of diary entries in this case covered wrestling with considerations that came as a result of having researched, and being concerned about, the area for a number of years. This method is unlikely to yield similar responses from non-expert participants.

Being able to add in artefacts was another benefit of having a relatively unstructured reporting setup. As previously reported by Hong et al. (2020), keeping artefacts exclusively digitally was not practical for ensuring inclusion and consideration in the wider diary entries, so needed to be printed to ensure this happened. The artefacts were of particular value, however, in bringing the outside world into the home, and reminding the researcher of the wider cyber security environment. Again, the chance nature of seeing news items, or social media posts were reminders of the researcher's framing of the world — would an average user see these posts, or regularly read the news sources that the person performing the diary study considers part of their everyday life?

The lack of instances of cyber security arising in day-to-day life, coupled with the finding here that organisations typically aim support at parents in relation to online safety — and that parents and children themselves discuss online safety when cyber security is asked about, as described in Chapter 4.3.2 — suggests that a diary study would not produce the insight needed to further the fourth RQ. This is particularly the case when reflecting further on the fact that generalised cyber hygiene and security methods made up a proportion of the instances reflected. The specific cyber security of home IoT devices was not the only thing considered, even in this context. It can be inferred from this that there is likely to be a more active way of interacting with families, to ensure that instances where cyber security can be related to home IoT devices are made clear.

RF 9: Solving cyber security issues can be uncomfortable and hard

Even though performed in a period of enhanced social distancing measures as a result of the COVID-19 pandemic, the diary study allowed for reporting not only of interactions with the researcher's nuclear family, but also gave an interesting insight into how the external world encroaches into the home. Prior research has already shown that individuals can find negotiating shared security difficult, even when there is prior agreement as to the importance (Watson et al. 2020), and that bystanders pose a particular set of security questions when considering home IoT devices (Windl and Mayer 2022). However, the lived difficulty of these situations may not be truly understood. To consider an example from the diary study here: the situation where the relative may or may not have had a compromised device with access to the researcher's home network allowed for exploring the difficulties of acting positively in emotive situations. If the victim of a security issue acts defensively, there is little that anyone else can do, even with a perfect knowledge of the theoretical steps to take.

RF 10: The language of cyber security is too complex for day to day interactions with non-experts

Involving young children is hard. We know that adults and children often use different languages to talk about cyber security (Jones et al. 2019), but when the concepts are too complex or too abstract for either the adult to explain or the child to understand, how is that knowledge transfer expected to happen? The diary entries provided space for reflection on how frail the concept of security within the home could be, and that hoping for users to manage this themselves is hard. Some of the artefacts — school curriculum and text books — helped to put the inability to talk about this with the children into context: as much as the researcher and her husband could not find the words for the cyber security issues they tried to discuss with their children, so the educational system does not set children up to learn about it in enough depth. It also underlines that even when children have parents who understand the reasons for and means of promoting good cyber security in the home, they will not necessarily find the opportunity for discussion and learning at home.

5.4 Limitations

There were many alternative paths that this research step could have taken. Both pieces of research followed directly from observations in Chapter 4, that turning to the Internet was a key means of answering questions and solutions and that the families involved showed a lack of awareness in relation to home IoT device security. These two pieces of research could have been replaced by others: discussions with experts about appropriate device security methods might have provided a cleaner list of what the key piece of advice should be, a more active outcome heading into the final piece of research. The website review also reflects a specific point in time, and possibly a specific framing of the Internet: although every effort was taken to anonymise the researcher's Internet connection to avoid finding results based upon her preferences and prior search history, this may have not been possible. Indeed, people searching for this information may well be sent to particular results based upon their search history and personal opinions of websites — which obviously cannot be accounted for in a review such as this one.

Not engaging further with families, but deciding to do a solitary, reflexive piece of work could pose the risk that, in entering the final piece of research, the abilities of families had not been taken into account in general. If families had been involved in a cognitive walkthrough, for example, to allow the researcher to watch them as they decided how to secure the device, it could have been possible to better grasp the specific problems that the families involved may have had, rather than focus on inferring what may be the issues, based on reflexions of the researcher's own life.

5.5 Conclusion

This chapter reported on two pieces of research that looked to provide answers to RQs 2 and 3, "What knowledge is available online to those who wish to implement cyber security measures for home IoT devices?" and "How can the researcher effectively understand the awareness and motivation to consider the cyber security of home IoT devices shown by families? ". It was prompted by using key pieces of information provided in the interviews and surveys about the behaviour of the majority of those individuals involved: they had no specific knowledge about cyber security for specific home IoT devices before or during ownership of those devices, and, should there be concerns, they would turn to the Internet for information; there was also little discussion between parents and children about cyber security.

The cyber security information review found that it is incredibly hard for users to search the Internet for information that is going to just work for them. Without additional prior knowledge, and in some cases, wider understanding of how home IoT devices fit into the wider home network, it is unlikely that a user would be able to pinpoint the most appropriate information to manage their specific threats.

The autoethnographic diary study provided a more reflexive background to this. Cyber security is a topic that is rarely top of mind, even in households with experts. Home IoT device use does not ordinarily prompt ongoing discussions about how to manage potential threats to both active and passive device users, and if issues do arise, they are often too complex to understand, fix or discuss.

How, then, can we hope to understand the best way of supporting families to manage the threats and risks posed by the home IoT devices that they currently own, or will own in the future? All the pieces of research so far have shown how little cyber security naturally comes up as a concern in the average household, with the autoethnographic diary method highlighting this, when considering the sparsity of diary entries — even in an interested household. These two pieces of research allowed for further reflection upon how to move families around the steps of the TTM cycle: if the information that they can easily find is not robust, and the home setup is not conducive to learning about appropriate security measures — or even knowing how to discuss the need for cyber security measures, how could an intervention bring in training and education at an appropriate level — and would families engage with the concept, if they had never previously considered it?

As such, getting to a point of understanding necessary interventions needed to improve the understanding of the average family requires something more active than reviewing their day-to-day activities through a diary study. The final piece of research will have to force a change in order to make families consider cyber security, to require — and thus subsequently help — them to think through those cyber security issues that matter to them. One method that has worked successfully in other areas of cyber security is that of serious gameplay, as it may allow, in this case, families to work through cyber security problems that may arise in the home without having to have gone through the lived experience first. By placing families in a safe situation where they can be helped to understand the threats and risks more clearly, as might affect them, they may be able to more clearly understand and act upon the ways in which they can keep their home IoT devices secure. This situation will also show the ways in which families either do not understand, or consider there to be enough value in pursuing specific solutions. Both outcomes will help answer the final RQ: "How can a board game act as an intervention to support families to move forward in their journey through the stages of TTM?"

Chapter 6

The creation of an intervention to promote positive cyber security actions amongst families: background and setup

6.1 Introduction

The research in the previous chapters has shown that despite using home IoT devices in their everyday lives, families are not aware of the potential threats that the devices may cause them; should they try to find out, they will typically not be able to find specific enough advice to make a clear difference. And even if they do feel happy enough to try and discuss cyber security within their families, or with others, they may well struggle to find the words to have a meaningful conversation. This means that there is a need to implement adequate training and education to support awareness in the participating families. The prior pieces of research have shown the place of most families on the TTM cycle — the hope with this final piece of research is to provide tools for participant families to move to the next stage — contemplation of using cyber security measures. As is shown in Figure 6, if the game can harness the right information at the right level to bring participant families to a level of contemplation, by raising their awareness of the subject, this is a good start around the cycle. Ideally, the game would also help participants further around the cycle — the lighter green sections of preparation and action, as a result of being given enough knowledge and feeling sufficiently empowered by the game to make a change.

All of these issues led to this thesis' final piece of research, as covered in this and the subsequent chapters. As mentioned in Chapter 5.3, initially it was considered that a means of getting to a point of finding the outcomes of RQ4, how can a board game act as an intervention to support participant families to improve awareness in relation to the cyber security of home IoT devices that they own and use?, might be to start with a diary study for families, similar to that seen in Garg and Sengupta (2019); Chalhoub et al. (2021); Williams et al. (2019). The findings from that piece of research, however, made it clear that it was unlikely that a diary study would garner the types of insight needed — or frankly, maybe any entries at all from participants.

As such, the decision was taken to pursue a method that would ensure that participants engaged with cyber security, rather than trying to capture their views passively, through a diary. This would allow for the active introduction of training and education exercises. Within the field of cyber security, serious games have been used as a means of explaining complex processes and implications for many years. In particular, there seems to be an inclination towards using the games in corporate settings as tabletop exercises. As explored in Haggman (2019), these "wargames" can offer immersion that allows participants to think through how their recovery from attack, initial setup of systems or product development may work. Within this field, however, games are less common when considering technology in the home, and there appears to be no games that focus upon the family as the target playing group.

The idea of a board game may be a well-trodden path in cyber security, yet getting to a game that is enjoyable and playable, alongside delivering the appropriate learning messages, is a complex skill, and one that the researcher could not claim to have in any meaningful way. As such, it felt necessary to split the research up to look at different elements of the progress and usefulness of the game. User-centred design (UCD) is not uncommon in the HCI and CSCW fields, where the participation of end-users in the design of a product is considered likely to create better end results. Many pieces of UCD research focus on the process and result of the application of the process, as well as the outcome (for example, Yao

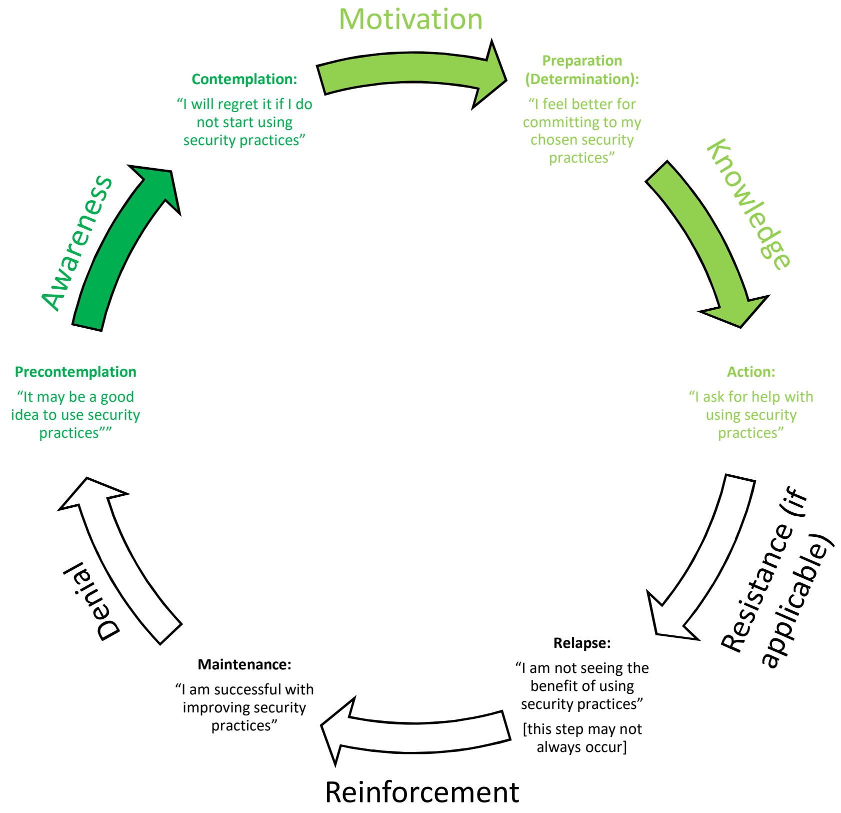

Motivation
Contemplation:
“I will regret it if I do not start using security practices”
Preparation (Determination):
“I feel better for committing to my chosen security practices”
Knowledge
Action:
“I ask for help with using security practices”
Resistance (if applicable)
Relapse:
“I am not seeing the benefit of using security practices”
[this step may not always occur]
Reinforcement
Maintenance:
“I am successful with improving security practices”
Denial
Precontemplation
“It may be a good idea to use security practices””
Awareness

Figure 6: The stages of TTM that the game hoped to support participant families through: at least to contemplation – if not also through to preparation and action. As adapted from Faklaris, Dabbish and Hong (2018)

et al. (2019a)) — as such, there are two main parts to this final piece of research, UCD, and active engagement with families for learning.

This leads to three sub-RQs as a means of breaking down the ways that the research can address RQ4. All sub-RQs rely upon outputs from the family to measure changes made. RQ4a will be measured by looking at the rating (out of 5) and written feedback provided by families in the week after playing the game. RQ4b will look at the written evidence collected from the families as part of the pre- and post-gameplay exercises. RQ4c will look at the feedback that the families provide about the week following gameplay.

RQ4a: Can UCD with families create an increasingly engaging board game that increases awareness of cyber security?

RQ4b: Do families understand a wider range of threats and risks of using home IoT devices after playing the board game?

RQ4c: Do participant families make changes in the cyber security methods they use at home in the period after playing the game?

These sub-RQs can provide evidence for answering the main RQ in a number of ways. It could be that the game itself is shown to be a useful training and educational tool to raise awareness amongst those families that take part to learn and rethink their cyber security at home, as well as spark conversation between parents and children. Alternatively, it could be that a game will not help, and the conclusion that could be taken from that, coupled with the other research in this project, is that cyber security management in relation to home IoT devices is too complicated or complex for users, and so the interventions need to happen before the devices arrive in the home. Or it could be a mixture of both, with some solutions resonating more with participants, and others less, so more nuanced observations can be made.

It is also important to bear in mind the model of TTM as described in Chapter 3 and Figure 1. Prior research has shown that many, although not all participants, are in a stage of precontemplation, in relation to cyber security of home IoT devices: that is, they have not considered it something that they need. When discussing more general forms of cyber security in Chapter 4, some participants showed signs of slipping into resistance or relapse in terms of the model — not being convinced that the effort being put into cyber security was worthwhile. Although more specifically focused on home IoT device use, this game will look, specifically, to see if those participant families that exhibit signs of being in a precontemplative stage at the start of gameplay move through the contemplation, preparation, and even action stages of the TTM cycle (Figure 6). Evidence of the game raising awareness, to get participant families to a point of contemplation will be evidenced through witnessing engaged discussion about the scenarios and cyber security methods presented in the game. Motivation leading to the stage of preparation to make security changes will be shown in the families of the participants making a positive group decision to try to implement cyber security measures that will support the use of their IoT devices at home. Finally, the game will show that it supports a movement into action if participants' families report making a change in their cyber security setup during the week following the game play. Given the time span of the research, it will not be possible to test the rest of the cycle (relapse/maintenance).

This chapter is structured in the following way. Section 6.2 will detail the research plan and the methods used. Section 6.3 will then go on to provide details as to how and why the first version of the game was designed, building upon principles of game design and past research. The findings and discussion will be found in Chapter 7.

6.2 Methods

This section will detail out the methodological process behind the entire piece of research. The methodology in and of itself is somewhat intricate, involving both gameplaying participant groups and control groups (as seen in Williams, Nurse and Creese (2019)), but also considering the sub-RQs which focus on both UCD and the improvement of cyber security knowledge. This section will explain the details of the structure of the research and the recruitment of participants.

6.2.1 Inclusion criteria

There were two participant groups within the study: a gameplaying group (the group participating in gameplay), and a control group (participating only in providing specific details, through online surveys, about cyber security behaviour and awareness). For both the gameplaying and the control groups, the inclusion criteria remained the same. In both cases, the invitation to participate was made to one parent, on the understanding that they:

- Lived in the UK
- Had at least one home IoT device at home, including either a smart TV, and/or a smart home assistant, and/or a streaming device
- Had at least one child aged between 11–18 living at home (in line with the broader ideas of what this may mean as discussed in Chapter 3.6). Other child(ren) could be of any age.

Unlike the interviews and surveys that had gone before, it was decided to target families that had at least one child of secondary school age[1] (with other children being of any other age). Having at least one child of this age was decided as an inclusion criterion for several reasons. Practically, it was thought that children of this age would have an understanding of how board games worked, and so gameplay would not be hindered simply through a lack of understanding of what was happening, or a lack of interest because of such a lack of understanding. Secondly, having received a number of years of primary school curriculum about cyber security or staying safe online would produce a level of awareness of the matters broached in the game, even if not a thorough understanding.

The decision was taken to have ten families participate in each round of playing and to aim to have around 100 control participants per round. Much like the research in Chapter 4, the idea behind this was to gain a breadth of answers from the control participants, given the high-level nature of the questions and the depth of consideration and experience from the gaming families. This may raise questions in terms of statistical power of comparison, given the unequal sizes of the two groups (Oldfield 2016). As discussed in Guo and Luh (2013), however, in this case, resources, in terms of time, money and participant interest, were such that more than ten families per session would have been impossible, whereas the short length of the control questionnaire allowed for a larger number of control participants to be sought. Given the fact that the number of gameplay participants were so small that in depth statistical analysis could not be reasonably applied, having the ability to review a larger number of control responses using more descriptive statistical measures felt appropriate.

6.2.2 Structure of the research

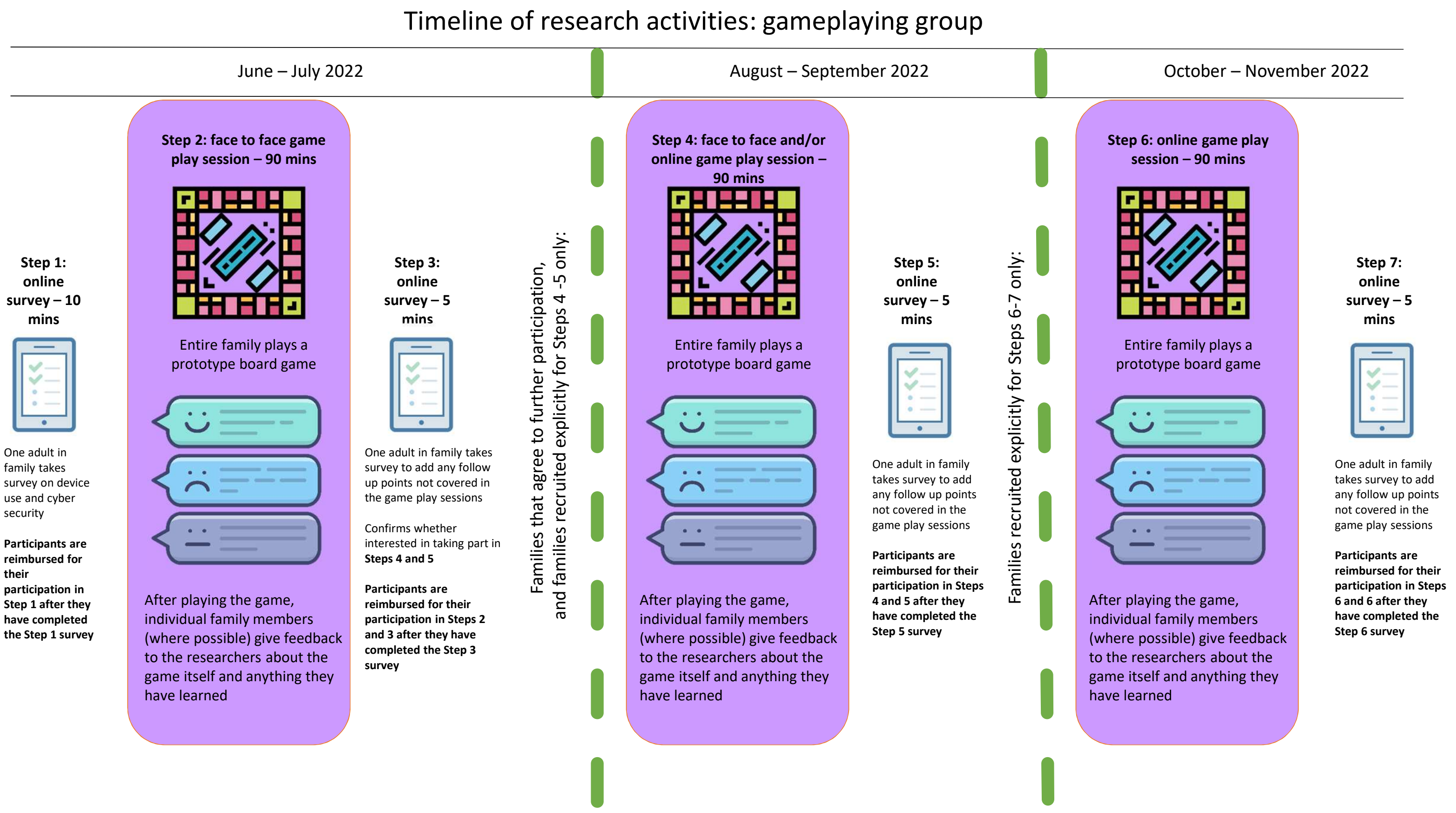
The research process undertaken with the two groups is detailed in Figures 7 and 8, respectively. For ease of narrative, the processes will be described below independently, but the timelines referred to in each ran concurrently during the course of the study.

Two surveys on Prolific were run initially: one to help find participants for the gameplaying group, the second to find participants for the control group. These

[1] 11-18 years old.

initial surveys took around 15 minutes to complete. The questions were the same for both gameplaying and control groups except the final question (which, in turn, asked about interest in participating in gameplaying sessions or control surveys respectively), covering aspects of device use and cyber security awareness and understanding in the home. The full list of questions asked can be found in Appendix J. As well as using the surveys as a means of finding participants, the survey was considered useful as a means of understanding whether sentiments and usage of devices had moved on since the initial survey in 2020. The findings from the survey are detailed out, and contrasted with the findings of the 2020 survey, in Chapter 4.

All participants completing surveys on Prolific (both the initial survey and three subsequent control surveys) were paid pro rata for their time for the initial survey, using the UK's Living Wage Foundation's 2021/2022 rate of £9.50 per hour, as it was at the time of receiving the favourable opinion from the university's ethics committee CREAG for the research in December 2021 (Living Wage Foundation 2022). All gameplay participants received an Amazon voucher for participating: those 18 and over received £30 per gameplay session, with those under 18 receiving £20 per session. Where applicable, participants that travelled to sessions were entitled to claim back costs associated with that travel based upon the university's standard rates.



Timeline of research activities: gameplaying group

June – July 2022

August – September 2022

October – November 2022

Step 1: online survey – 10 mins

One adult in family takes survey on device use and cyber security

Participants are reimbursed for their participation in Step 1 after they have completed the Step 1 survey

Step 2: face to face game play session – 90 mins

Entire family plays a prototype board game

After playing the game, individual family members (where possible) give feedback to the researchers about the game itself and anything they have learned

Step 3: online survey – 5 mins

One adult in family takes survey to add any follow up points not covered in the game play sessions

Confirms whether interested in taking part in **Steps 4 and 5**

Participants are reimbursed for their participation in Steps 2 and 3 after they have completed the Step 3 survey

Families that agree to further participation, and families recruited explicitly for Steps 4 -5 only:

Step 4: face to face and/or online game play session – 90 mins

Entire family plays a prototype board game

After playing the game, individual family members (where possible) give feedback to the researchers about the game itself and anything they have learned

Step 5: online survey – 5 mins

One adult in family takes survey to add any follow up points not covered in the game play sessions

Participants are reimbursed for their participation in Steps 4 and 5 after they have completed the Step 5 survey

Families recruited explicitly for Steps 6-7 only:

Step 6: online game play session – 90 mins

Entire family plays a prototype board game

After playing the game, individual family members (where possible) give feedback to the researchers about the game itself and anything they have learned

Step 7: online survey – 5 mins

One adult in family takes survey to add any follow up points not covered in the game play sessions

Participants are reimbursed for their participation in Steps 6 and 6 after they have completed the Step 6 survey

Figure 7: Research process: gameplaying group

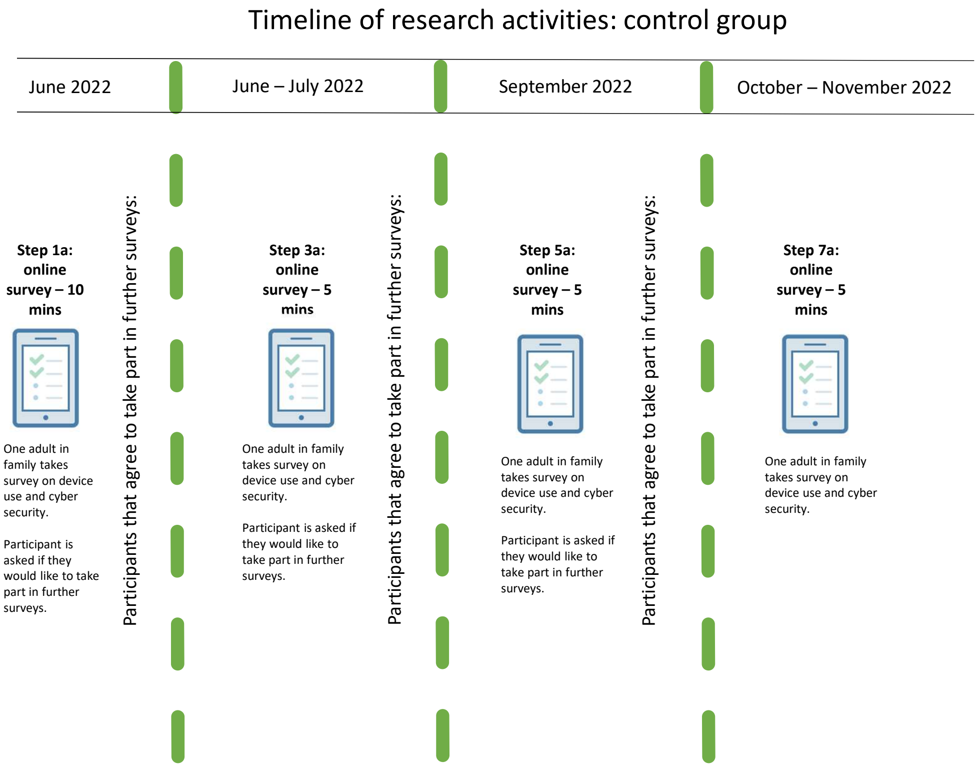

Timeline of research activities: control group
June 2022
June – July 2022
September 2022
October – November 2022
Step 1a: online survey – 10 mins
One adult in family takes survey on device use and cyber security.
Participant is asked if they would like to take part in further surveys.
Participants that agree to take part in further surveys:
Step 3a: online survey – 5 mins
One adult in family takes survey on device use and cyber security.
Participant is asked if they would like to take part in further surveys.
Participants that agree to take part in further surveys:
Step 5a: online survey – 5 mins
One adult in family takes survey on device use and cyber security.
Participant is asked if they would like to take part in further surveys.
Participants that agree to take part in further surveys:
Step 7a: online survey – 5 mins
One adult in family takes survey on device use and cyber security.

Figure 8: Research process: control group

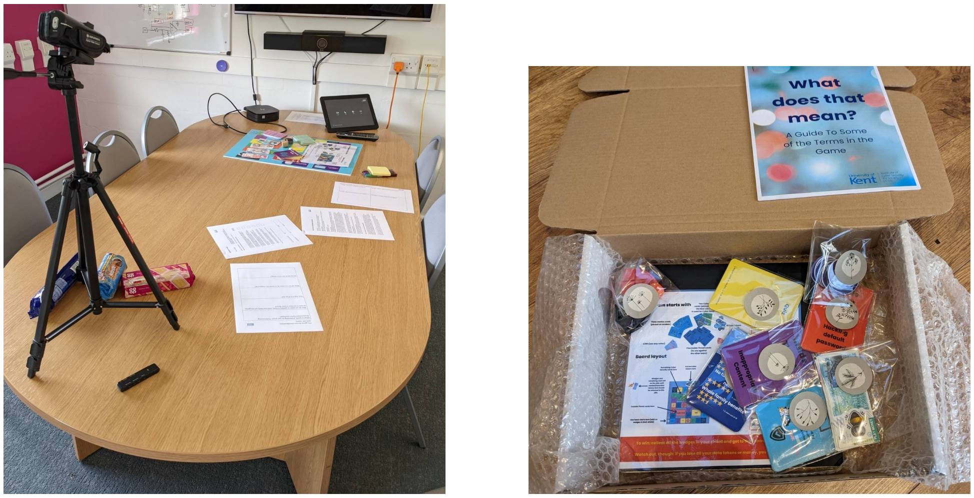
6.2.3 Gameplaying group process (Figure 7)

Participant recruitment (Step 1)

As mentioned in the previous section, a survey promoted through Prolific was used as the primary way of recruiting participants willing to take part in the gameplay process (Step 1 in Figure 7). Participants were also sought through the researcher's professional and personal networks.

Gameplay sessions (Steps 2, 4, 6)

Steps 2, 4 and 6 were the gameplay sessions. The structure of the sessions remained the same, regardless of the round. Steps 2 and 4 involved in-person sessions: these sessions were held in London and Kent, with families travelling to locations in each area to participate. Steps 4 and 6 also involved online participants. Online sessions were agreed in advance: the researcher sent out a copy of



(a) Setup of in-person session

(b) Materials sent to online participants

Figure 9: In-person setup and online participant package

the board game, instructions and all documentation to participants via courier in the days leading up to the session. The session then happened online, using Microsoft Teams. Both on- and off-line, the sessions ran in the same way as described below. The three rounds of gameplaying sessions were separated by a few weeks, where changes were made to the game itself, based upon the feedback of the participants in the previous round. As such, the first round of gameplay took place in June and July 2022. The second round took place in August and September, and the final round took place in October and November 2022. Figure 9 shows the in-person game setup and the package sent to online participants.

Once welcomed into the session, the family was then asked to split into two teams. Once this had been done, they were then asked to fill in the pre-game device consideration form in their teams (see Appendix K). The researcher explaining the task made it clear that the participants did not have to spend more than five minutes, in total, thinking and answering these questions, and that they could interpret the questions however they liked; this was done to try and get an understanding as to what would come to the top of mind quickly for the participants, and how they would interpret ideas around cyber security threats and risks in terms of the home IoT devices that they had.

Once participants had finished filling in that form, they were asked to play the game for thirty minutes. Across all rounds, participants were given all the game pieces, the board, and instructions, as well as a booklet of common terms to refer to in case of gaps in knowledge (see Appendix P). They were not told how to set up the board, just to take a few minutes to read the instructions before starting to play. If participants had questions as to gameplay, or could not work out how to progress gameplay, the researcher would step in to answer questions about how to progress. In the case of in person gameplaying sessions, researchers sat away from the family whilst they played to avoid interrupting too much; in online sessions, the researcher turned off video camera and microphone during gameplay unless explicitly needed to help further gameplay.

Gameplay was stopped after thirty minutes. The purpose of the game was to play for this period of time, rather than having participants engage with all the cards or some other metric. This was because, to some extent, the randomness of a board game would make it difficult to achieve complete coverage of the materials within a period of time that participants would continue to focus (particularly the children involved). Deciding to play the game for a set period of time also meant that the amount of time needed to complete the game was less of a concern, allowing for the possibility of more threat cards and cyber security cards, in particular, to be used. In two cases where participants finished the game within twenty minutes, they restarted and played again; in other cases, games either naturally finished at around the thirty-minute mark or — as was more often the case — the families were asked to stop playing once the time had elapsed. During this period, the participants were video and audio recorded as they played; as much as possible, the video focused on the board, not the participants, to capture any gestures or movements arising from gameplay. Other points arising from gameplay — confusion, areas of conflict or excitement, for instance — were captured on the audio recording and could be triangulated with the video recording if necessary. The video recording was stopped after the gameplaying session ended; audio recording carried on until the end of the session.

Immediately after playing, the family was asked — as a group, not as two teams — to fill in another form (see Appendix L), similar to the first, but with two different questions at the end, asking for potential cyber security measures they could adopt as a family, and what measures they did agree to adopt. As discussed in Denning, Shostack and Kohno (2014), the likelihood of a positive and engaged experience during gameplay means that the immediate post-gameplay period is the best opportunity to get players to reflect and agree to making changes. This piece of paper was then photographed by the researcher, so that the participant family could take it away as a reminder of their agreement.

The final stage of the gameplaying sessions was a semi-structured interview. The interview, in rounds one and two, covered two main topics: firstly, what they felt worked, and did not work, with the game, and how they might improve it. Secondly, what they felt they had learned from playing the game: what had they known before, what had they not, had anything surprised or confused them? The full list of questions are in Appendix M. In the third round of gameplay, where there was no formally planned next stage of improvement, the interviews focused on the second question set, albeit with further gameplay suggestions coming out as part of the observed gameplay and answering of the questions. In total, sessions lasted between 60–90 minutes.

During the interviews, all members of the family were addressed together. This stage of the session often occurred nearly an hour into the entire session, and so younger children had often become a bit disengaged at this point. This was not necessarily a problem, however: in the in-person sessions, they were encouraged to move around the room, play with the game pieces, doodle on paper as well as have drinks and snacks, both of which were provided, to help keep their interest. Online sessions allowed for younger children to come and go as they pleased in their own home. In both setups, parents would ask their children's views on questions being asked: often they may make the questions more directly applicable to what they knew their children would understand in a similar way to that exhibited in the interviews in Chapter 4. These modifications would increase the likelihood that the children might still answer questions despite starting to tire.

There were three rounds of gameplay in total, each having ten families participating. Table 16 details out the makeup of all participant families. The first round was held exclusively in person, in locations in Kent and London, in June and July 2022. There were 14 adults (over 18) and 23 children (18 and under) participating, as detailed in Table 16. The average age of the children was 11.43 years (SD 2.73); the youngest was 7 and the eldest 18.

The second round had seven in-person families and three online families, in August and September 2022. The seven in-person families were all families from the first round who had been invited back to see if the game had improved, round-upon-round,[2] with the three online families being new families, with no prior knowledge of the first version of the game. As before, the in-person gameplaying sessions took place at a location in Kent or London; the online participants were based in various locations in England. There were 17 adults (over 18) and 19 children participating in the second round, with one family having one fewer sibling taking part in the second round than the first. The average age of the children was 12.32 years (SD 2.87); the youngest being 7 and the eldest being 18.

The third round had ten online families, in October and November 2022. Families participated from all areas of the UK, with representation from each of the devolved nations. Each family only participated in the third round: no participants had been involved in earlier rounds. There were 18 adults (over 18) participating in the third round, and 19 children. One family expected an older sibling, aged 15, to participate, but who refused to immediately before the start of the session. The average age of the children was 12.21 years (SD 4.00); the youngest being 6 and the eldest being 17.

[2] All families that participated in the first round were invited back for the second round, with three declining to do so.

Table 16: Game participants

Round	Family code	Location	Number of adults	Child 1 age	Child 2 age	Child 3 age	Child 4 age
1	K1	Kent, England	2	14	13	9	
1	L2	London, England	2	11	8		
1	K3	Kent, England	1	12	10		
1	L4	London, England	1	11	8		
1	K5	Kent, England	1	15	14	12	
1	L6	London, England	1	12	9		
1	L7	London, England	2	15	10	7	
1	L8	London, England	2	13	11	9	8
1	L9	London, England	1	18			
1	L10	London, England	1	14			
2	L6	London, England	1	12	9		
2	L9	London, England	1	18			
2	K1	Kent, England	2	14	13	9	
2	K3	Kent, England	1	12	10		
2	O1	Online — Birmingham, England	2	13	11		
2	O2	Online — Birmingham, England	2	14	12		
2	L10	London, England	1	14			
2	O3	Online — London, England	3	17	15		
2	L7	London, England	2	15	7		
2	L2	London, England	2	11	8		
3	O4	Online — West Yorkshire, England	1	15	12	6	
3	O5	Online — Bedfordshire, England	**3	16			
3	O6	Online — Airdrie, Scotland	1	9	*15		
3	O7	Online — Derbyshire, England	1	18	17	14	14
3	O8	Online — Cleveland, England	2	12	9		
3	O9	Online — Arbroath, Scotland	2	12	8		
3	O10	Online — Peterborough, England	2	12	10		
3	O11	Online — Newtownards, Northern Ireland	2	11	9		
3	O12	Online — Pontypridd, Wales	1	17	14		
3	O13	Online — Wolverhampton, England	2	15			

* Indicates child decided not to take part at time of gameplaying session

** Indicates grandparent also took part in gameplaying session

Follow-up surveys (Steps 3, 5, 7)

A week after the survey, the corresponding adult from the family was sent a follow-up survey. The survey asked for any further reflections about the board game, and if any family members had participated in any training, or seen any news about cyber security, in the past week. Finally, they were asked if they had modified any cyber security settings in the home as a result of playing the game. For these questions, see Appendix N.2. Participants were sent the survey a week after the session, and reminded up to four times to fill in the survey, over a two-week period following the initial request. All but one participant family filled in the survey (that is, the survey was filled in in 29 out of 30 instances). Once the survey had been filled in, the researcher sent the participants the Amazon vouchers promised as reimbursement.

6.2.4 Analysis of gameplaying sessions

The data generated from the sessions was recorded and analysed in various ways. During the gameplaying sessions, participants were given the opportunity to take notes to raise during the interview about gameplay, although, in practice, only one family did. The researcher also took notes of aspects of gameplay that may have needed further discussion (whether because they were problematic, raised questions or alternatively, seemed to work well); similarly, the researcher took notes as to the reactions that participants had to certain cyber security measures, scenarios or devices, to ensure that they were covered in the interview after gameplay had finished. This ensured that issues were covered without interrupting the flow of gameplay. Interviews were transcribed and subsequently coded by two researchers using MaxQDA. Because the coding process was aimed at gaining insights into specific topics — namely those around improving gameplay and cyber security understanding and learnings — codes were set up prior to the coding taking place, allowing for deductive analysis, following Braun and Clarke (2021). Both researchers coded the texts against the code book, reviewed the outcomes, and discussed points of disagreement before performing a second round of coding. Inter-rater reliability was calculated based upon this second iteration of coding, and was calculated to have a Cohen's *kappa* value of 0.64, indicating a substantial level of agreement. The full code book can be found in Appendix O.

In addition to the interview transcripts, the two forms filled in — the pre- and post-game consideration sheets — were also transcribed and coded, again using MaxQDA. This coding tagged every answer to the questions in both the pre- and post-game forms, given as they were, objective things being listed out (such as “Hackers”, “personal data”). This enabled a comparison of the types of threats listed before and after gameplay. It also allowed for comparison of these answers against the final survey question asking what changes the participants had made in the week following the gameplay.

Control group process (Figure 8)

Although other cyber security-focused board games have been researched without setting up a control group for comparison (e.g. Haggman (2019); Frey et al. (2019); Hart et al. (2020); Jaffray, Finn and Nurse (2021)) it felt important to have this step in place as an objective measure of the game’s impact. The use of a control group is important to understand whether any changes occurring in the gameplaying group has happened as a result of the intervention (that is to say, playing the game), or some other event. In this case, as previously described, a control group was sought using the Prolific platform, immediately before participants for the gameplaying group were sought (so as not to enable any potential control group participants to gain an understanding of the gameplaying element of the research). They answered the same initial survey as the respondents to the gameplaying survey, with the same inclusion criteria.

The intention of the control group was to recruit around 100 participants to fill in a survey identical to the final survey undertaken by the gameplaying participants, minus questions around gameplay, during the period in which the three rounds of gameplay were being undertaken. The questions can be found in Appendix N.3. Surveys were sent out to the control groups in June, September and October 2022, and were kept open until the last gameplaying survey was received back. These surveys relate to Steps 3a, 5a and 7a in Figure 8. This was decided as the most practical approach to setting up the control group, rather than, as has been seen in other research, creating an identical game with no specific security focus (Williams, Nurse and Creese 2019); with this particular game, not only would the creation of the game without a focus on cyber security be extremely hard to achieve, but would have been logistically difficult and prohibitively expensive to recruit thirty more families to participate.

Control participants were asked to comment on four different questions. Had they, or anyone in the household: bought any new devices, had any cyber security training, seen any cyber security news stories, or made any changes to their cyber security setup in the home. The initial survey asked if this had happened in the last month, and the subsequent surveys asked if it had happened in the last 4–8 weeks (roughly the period between surveys being sent out). After answering these questions, participants were given the option not to participate in the subsequent surveys. This led to a drop in participants between the first (115 participants) and second surveys; the second and third surveys had the same number of respondents (97). One participant was removed from the analysis of the first and second surveys (and not invited to take the third survey) after identifying themselves as part of a gameplaying family.[3]

Analysis of control data by itself, and with gameplaying data

Given the relatively small amount of data generated from these surveys, they were analysed using, on the whole, descriptive statistics. The findings were then compared with the same questions answered by the gameplaying participants. Although the small number, and differing numbers between control and gameplaying groups may make statistical analysis a somewhat questionable comparative approach, chi-squared tests were undertaken as a means of providing somewhat more rigour to the final analysis as to the differences, if any, exhibited between the groups. This will be explored in Chapter 7.

6.3 Initial game design

In order to understand the starting point from which the UCD activity began, it is important to look in detail at the process of creating the initial version of the game. Although this version of the game subsequently changed significantly — and the ways in which this happened will be detailed out in Chapter 7 — the underlying principles of the core learning aspects remained the same throughout the rounds of gameplay and improvements.

[3] This participant's spouse had independently filled in the gameplaying questionnaire.

Serious games have been described as "games [with] an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement" (Abt 1987). Marczewski (2018) further described the type of game being designed here as a *Purposeful* game, seeking, as it does, to have some form of "real-world outcome". In this case, the hoped real-world outcomes would be an amelioration of the areas of deficit or confusion that may arise, based upon the *RFs* from earlier on in the project.

Table 17 gives a list of the findings and the decisions that were taken in order to incorporate them into the initial design. Several of them focus upon the importance of making scenarios and ideas brought up in the game relatable to a player's home context, which covers both aspects of using clear and simple language, as well as proposing potential understandable measures, and promoting wider discussion among all — or the majority of — the family members playing the game. The decisions noted in Table 17 were made, in part, as a result of understanding the limits of understanding that families had exhibited in the previous pieces of research.

Table 17: Mapping research findings to underlying game principles

Number	From piece of research	Research Finding	Initial Game Solution
RF 1	Interviews and Survey	Families are happy to use devices, particularly Smart TVs and Smart Home Assistants, without proactively considering security	Limit the game focus to the most common devices of Smart TVs and Smart Home Assistants Use examples of potential cyber security issues that have impacts on Smart TVs and Smart Home Assistants
RF 2	Interviews and Survey	Families do not have a clear understanding of the threats and risks their devices may pose	Use examples of the different types of cyber security threats as they apply to Smart TVs and Smart Home Assistants Make threats — including potential for negative outcomes — explicit in outcomes of gameplay
RF 3	Interviews and Survey	There is a lack of opportunities for learning for both adults and children	Use a number of mechanisms within the board game to engage in learning
RF 4	Interviews and Survey	Parents model behaviour promoting careful use of devices, the importance of saving money and understanding consumer protection frameworks — but not security	Use the game mechanics and story to explore the different impacts of focusing upon certain aspects of device use over others, and the risks that this may incur
RF 5	Cyber Security Information Review	Users need to understand what is a threat to them specifically to apply any cyber security information they might find	Present players with a number of potential threats to their home or device in the game: make such threats relatable and memorable.
RF 6	Cyber Security Information Review	Information about device security likely needs wider context to be accurately applied	Use game mechanics to allow players to reflect on their own devices, network equipment and home setup with other family members.
RF 7	Cyber Security Information Review	Hard to find credible guidance	Use credible sources as the basis of all aspects of the game
RF 8	Autoethnographic Diary Study	Cyber security rarely arises in every day device use	Provide a range of scenarios that are sufficiently engaging to allow players to reflect upon and remember the scenarios, as well as providing meaningful, and actionable, measures
RF 9	Autoethnographic Diary Study	Solving cyber security issues can be uncomfortable and hard	Provide a range of scenarios that are not overly technical or daunting to allow for discussion Provide simple examples of cyber security steps that could be taken in general rather that in specific situations
RF 10	Autoethnographic Diary Study	The language of cyber security is too complex for day to day interactions with non-experts	Use language carefully in the game Provide explanations as part of the game documentation

Despite the primary goal of a serious game to “not have entertainment, enjoyment or fun as their primary purpose” (Michael and Chen 2005), it is vital to balance the desired learning outcome with sufficient enjoyment for participants to feel some sense of flow whilst playing (Csikszentmihalyi 1990). Flow is a state of involvement in an activity where those feeling it may forget external aspects (in this case, that they are taking part in research, that they are being watched whilst they play, that it is not a professionally designed board game) and simply enjoy the task at hand. As Prensky (2007) pointed out, enjoyment in game participation makes learning from that game more likely. This requires significant consideration to be given as to the design and delivery of the game.

The first element to be considered is the medium of the game. In an age where games are as likely, if not more so, to be electronic than physical, why a board game? A board game layout provides for a physical set up of participants: unlike a computer game, or even a card game, participants have to be sat around a board, engaging with the game as a group (both as a whole, but also within the teams). This gives an opportunity for groups such as families to concentrate on the topics raised in the game, a crucial aspect of serious game engagement. A game based around the movement of pieces around a board, with a number of potential types of action based upon where the pieces land, allows for a more complex series of actions and possible areas for learning than, say, a card-based game. Hart et al. (2020) found that having a board increased player engagement over the use of just cards: players could use the board as a visual reminder of the game’s story throughout the playing session. As discussed by Haggman (2019), albeit about the marginally different example of cyber wargames, he lists many reasons why a physical boardgame provides for better outcomes than online or computer-based versions. These include aspects of modifiability, accessibility and affordability, but more importantly here, “ [w]hatever the granularity of a wargame, it can never simulate the real world with complete accuracy, yet the people who partake in the game are the same as they are in the real world. . . Wargaming is about exploring different paths through scenarios, but the final outcome of a game is perhaps less important than the process of getting there. Wargaming is a participatory activity where human action and interaction is central to the experience, and it is this experience which is one of the most important things a wargame can offer.” This is true of the experience required in this boardgame, where the joint actions, and interactions of the teams should lead to a collective understanding of how to improve, or at least agree upon, what are the most important things to consider as a family when it comes to cyber security of home IoT devices. This experiential action and interaction is clearly valuable in the cyber security context, as a number of recently developed serious games in the field have been board or table-top in nature — for examples, see Hart et al. (2020); Gondree and Peterson (2013); Denning, Shostack and Kohno (2014); Frey et al. (2019).

In his book the *Art of Game Design* (Schell 2019), Schell recommended considering game design through a number of lenses, or pertinent questions, that help to frame the players' — and developer's — hoped experience through making and playing the game. Although not limited to board game development, a number of these lenses are important in helping to clarify the ways in which the game should achieve its aim. A fundamental lens is that of the *Elemental Tetrad* — namely, for a board game to be engaging, it must meld four particular aspects: *mechanics* (the procedures and rules of the game), *story* (what unfolds throughout the game), *technology* (that is to say, how users are enabled to do things in the game — the medium by which the aesthetics take place) and *aesthetics* (how the game looks and enables immersive gameplay). These four elements will be considered below as a means of exploring the decisions made around the development of the first version of the game, used in round one of the gameplay sessions. It should be mentioned that, prior to playing the game with participants in round one, two pilot gameplay sessions were run within the university department, allowing for minor changes as detailed in the sections that follow.

6.3.1 Mechanics of the game

Schell (2019) describes "mechanics" of a game as the "core of what the game truly is...the interactions and relationships that remain when all of the aesthetics, technology and story are stripped away." This section will consider, then, the reasons behind core aspects of the first version of the game. These are broadly summed up as:

- How the game should function

- Types of learning opportunities

- Levels of knowledge, challenge, skill and chance

Working within the boundaries of expecting a family to play the game, it was immediately apparent that two teams would be the most appropriate number of teams to incorporate, to avoid, in most cases, having children too young to fully comprehend how to play on a team by themselves. As mentioned above, the decision was taken to use the two most common types of home IoT devices predominating household ownership in the UK (smart TVs and smart home assistants),[4] and would provide a level of specificity about the setting of the game that has been considered valuable in previous work (Frey et al. 2019; Hart et al. 2020). Having physical representations of devices likely present in the participants' home would allow for contextualisation of the issues faced in the game: such contextualisation is necessary to allow conversations and discussions to continue after the gameplay has ended (Gondree and Peterson 2013). In order to appeal to participants, and be easily understood in the time constraints of the research session, it was decided that the game should be recognisable in structure as a turn-taking game, where each team works their way around a board structure based upon a series of squares. Each square would contain a different activity for the team landing upon it to undertake. The game should be competitive between teams, based upon the avoidance of losing data or money (as further explained below); within teams, however, participants would have to work together to explore the activities. This would allow for discussion, but might allow for two potential issues: one, less helpfully, that more dominant family members, possibly with more knowledge, would take over all the gameplay, reducing general opportunities for learning by all (Frey et al. 2019); but two, it might bring out those with playing less competitive personalities. Zahir et al. (2015) found that women were typically less competitive when playing games — this may, of course, be the case for many participants, and so, whilst competition is a useful means of improving engagement, it must be balanced against more collaborative activities.

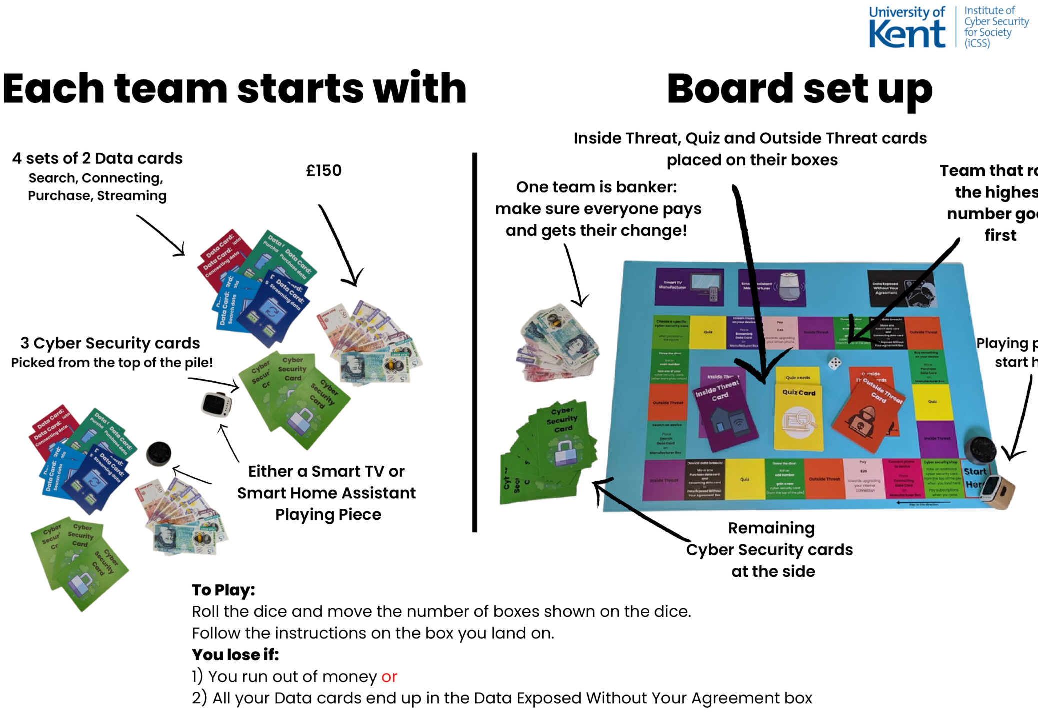
As a serious game, the mechanics of the game also had to ensure that the

[4] Although the previous pieces of research included streaming devices as well, the relative rates of ownership of smart TVs and smart home assistants are much higher. When considering the design of the game pieces, it was also recognised that the shape of a streaming device (as a piece of equipment to be plugged into a TV or similar) is not as immediately relatable as the other two device types.

learning opportunities needed were appropriately embedded within the fundamental gameplay. The fundamental aspects were considered to be a notion of

- Appropriate cyber security methods
- An understanding of the threat types arising from home IoT device use
- A mechanism to learn about other cyber security topics not directly linked to threat types
- A means of explaining the relative importance of the loss of both personal data and money from device use

Furthermore, as a serious game, the level of skill or knowledge entering the game would, ideally, be relatively low — too high and the learning opportunities may be limited; too low, and the concepts may make no sense. Gondree, Peterson and Pusey (2016) highlighted the importance of keeping players engaged by ensuring an appropriate level of difficulty. The game needed to be pitched at a level that would capture everyone in between the two ends of the spectrum: allowing for expansion of knowledge growth as the game progressed, and an element of challenge being involved in the progressing successfully through the game (rather than the activities being faced being too easy, or impossibly hard). Balanced with that, however, is a need to maintain a sense of chance within the game. A contradiction of poor cyber security measure is that sometimes, despite poor cyber security hygiene, users of devices are not meaningfully affected when bad things could happen. The element of chance — that the bad thing could happen, but might not, allows for participants to recognise the element of choice, and trade-offs, needed when planning cyber security strategies. The winning or losing of the game had to revolve around two key aspects of home IoT ownership — loss of money, and loss of data. Whilst loss of money is not necessarily a core cyber security consideration in and of itself, we know from *RF 4* that it is a core concern of users. Making the loss of money and the loss of personal data equivalent in gameplay could serve to elevate the status of personal data loss in participants' minds. Chance is represented in the game in aspects such as rolling the dice to determine the outcome of potential threats; it is also more directly seen in the inclusion of squares where, should you land on them, you lose data or money instantly.



Each team starts with

4 sets of 2 Data cards
Search, Connecting,
Purchase, Streaming

£150

3 Cyber Security cards
Picked from the top of the pile!

Either a Smart TV or
Smart Home Assistant
Playing Piece

Board set up

Inside Threat, Quiz and Outside Threat cards
placed on their boxes

One team is banker:
make sure everyone pays
and gets their change!

Team that rolls
the highest
number goes
first

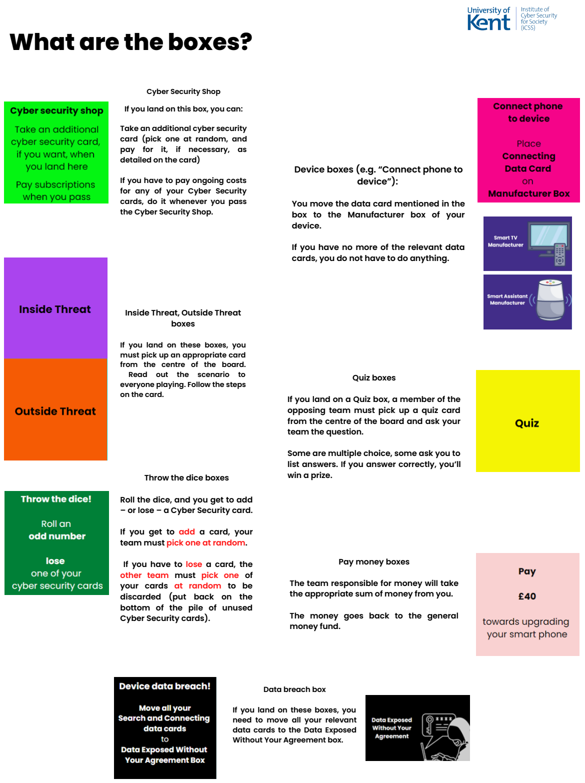
Playing pieces
start here

Remaining
Cyber Security cards
at the side

To Play:
Roll the dice and move the number of boxes shown on the dice.
Follow the instructions on the box you land on.
You lose if:
1) You run out of money or
2) All your Data cards end up in the Data Exposed Without Your Agreement box

Figure 10: Setup instructions for the first round of gameplay

With each version of the game, so the rules evolved to refine language, brevity and clarity to avoid disruptions to gameplay (Zahir et al. 2015). The rules provided to the participants in the first round of gameplay were separated into two key aspects: one document showed how to set up the board and pieces, how to avoid losing, and other fundamental steps (the direction to go around the board, who goes first and so on) — see Figure 10. The second document was to explain the activities for each square on the board — see Figure 11. Certain rules, such as how to perform the activity on each square, had to be followed carefully, whereas other, more norm-based rules (who goes first, direction of play) affected the game less, and so could be tailored as the players wished or according to what they were used to. A third piece of documentation was also provided to participants, a booklet with terminology in. For the full booklet, see Appendix P. This booklet was provided to all participants in every round, to help definitional questions that might arise. In the event, only two families used the booklet, and even then, it was after gameplay, to be used as an *aide mémoire* for future conversations.



University of Kent | Institute of Cyber Security for Society (iCSS)

What are the boxes?

Cyber security shop

Take an additional cyber security card, if you want, when you land here

Pay subscriptions when you pass

Cyber Security Shop

If you land on this box, you can:

Take an additional cyber security card (pick one at random, and pay for it, if necessary, as detailed on the card)

If you have to pay ongoing costs for any of your Cyber Security cards, do it whenever you pass the Cyber Security Shop.

Device boxes (e.g. "Connect phone to device"):

You move the data card mentioned in the box to the Manufacturer box of your device.

If you have no more of the relevant data cards, you do not have to do anything.

Connect phone to device

Place **Connecting Data Card** on **Manufacturer Box**

Inside Threat

Outside Threat

Inside Threat, Outside Threat boxes

If you land on these boxes, you must pick up an appropriate card from the centre of the board. Read out the scenario to everyone playing. Follow the steps on the card.

Quiz boxes

If you land on a Quiz box, a member of the opposing team must pick up a quiz card from the centre of the board and ask your team the question.

Some are multiple choice, some ask you to list answers. If you answer correctly, you'll win a prize.

Quiz

Throw the dice boxes

Throw the dice!

Roll an **odd number**

lose one of your cyber security cards

Roll the dice, and you get to add – or lose – a Cyber Security card.

If you get to add a card, your team must pick one at random.

If you have to lose a card, the other team must pick one of your cards at random to be discarded (put back on the bottom of the pile of unused Cyber Security cards).

Pay money boxes

The team responsible for money will take the appropriate sum of money from you.

The money goes back to the general money fund.

Pay

£40

towards upgrading your smart phone

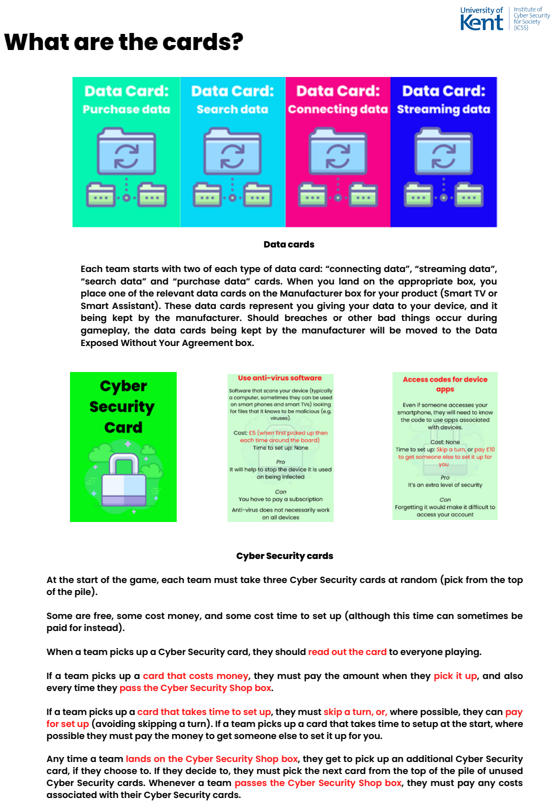
Device data breach!

Move all your Search and Connecting data cards to **Data Exposed Without Your Agreement Box**

Data breach box

If you land on these boxes, you need to move all your relevant data cards to the Data Exposed Without Your Agreement box.

(a) Page 1



University of Kent | Institute of Cyber Security for Society (iCSS)

What are the cards?

Data Card: Purchase data
Data Card: Search data
Data Card: Connecting data
Data Card: Streaming data

Data cards

Each team starts with two of each type of data card: "connecting data", "streaming data", "search data" and "purchase data" cards. When you land on the appropriate box, you place one of the relevant data cards on the Manufacturer box for your product (Smart TV or Smart Assistant). These data cards represent you giving your data to your device, and it being kept by the manufacturer. Should breaches or other bad things occur during gameplay, the data cards being kept by the manufacturer will be moved to the Data Exposed Without Your Agreement box.

Cyber Security Card

Use anti-virus software

Software that scans your device (typically a computer, sometimes they can be used on smart phones and smart TVs) looking for files that it knows to be malicious (e.g. viruses).

Cost: £5 (when first picked up then each time around the board)
Time to set up: None

Pro
It will help to stop the device it is used on being infected

Con
You have to pay a subscription

Anti-virus does not necessarily work on all devices

Access codes for device apps

Even if someone accesses your smartphone, they will need to know the code to use apps associated with devices.

Cost: None
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
It's an extra level of security

Con
Forgetting it would make it difficult to access your account

Cyber Security cards

At the start of the game, each team must take three Cyber Security cards at random (pick from the top of the pile).

Some are free, some cost money, and some cost time to set up (although this time can sometimes be paid for instead).

When a team picks up a Cyber Security card, they should read out the card to everyone playing.

If a team picks up a card that costs money, they must pay the amount when they pick it up, and also every time they pass the Cyber Security Shop box.

If a team picks up a card that takes time to set up, they must skip a turn, or, where possible, they can pay for set up (avoiding skipping a turn). If a team picks up a card that takes time to setup at the start, where possible they must pay the money to get someone else to set it up for you.

Any time a team lands on the Cyber Security Shop box, they get to pick up an additional Cyber Security card, if they choose to. If they decide to, they must pick the next card from the top of the pile of unused Cyber Security cards. Whenever a team passes the Cyber Security Shop box, they must pay any costs associated with their Cyber Security cards.

(b) Page 2

Figure 11: Gameplay instructions for the first round

6.3.2 The story of the game

This section will consider the high-level story behind the aspects of the game. Further details about the design of items mentioned here will be discussed in the sections on Technology and Aesthetics below.

The fundamental story within the game is that each team's objective is to retain as much money and data as possible, to avoid being out of money and/or having had all your data "exposed without your agreement". The core elements of story within the game are the types of activities that players land on as they go through the board. These elements arise out of the need to address the majority of the research findings (as detailed out in Table 17), and where possible, arise from real-world events or recommendations from trusted organisations. As such, scenarios and questions that appear within the game are all based upon at least one of four things: evidence from the previous research in the project; guidance from governmental sources and consumer protection agencies in the UK and US (these include NCSC,[5] FBI,[6] NIST,[7] Which?[8] and Consumer Reports[9]); reported cyber security incidents in widely available media sources and online support forums (those which are available to read online, in English, without a subscription or paywall); and academic research. Similarly, the cyber security tools available for use in the game are those recommended by governmental sources in the UK and US (NCSC, FBI, NIST) — this is to try to avoid the inclusion of tools being promoted by parties with a financial or other interest in their use. For a full list of the scenarios on the cards, and the reasoning behind them, see Appendix I.

There are two teams — one is the "Smart TV" team and the other is the "Smart Home Assistant" team. These team names are meant to help focus the participant's minds on their own smart TVs or home assistants (Gondree and Peterson 2013); in terms of the gameplay, the devices themselves are not particularly significant in that both are treated the same in terms of the scenarios and other aspects of gameplay. That said, at the point of the initial design, the intention

[5] https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

[6] https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot

[7] https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity

[8] https://www.which.co.uk/l/smart-homes-safety-and-security

[9] https://www.consumerreports.org/home-garden/smart-home/guide-to-smart-home-devices-tech-a1007276600/

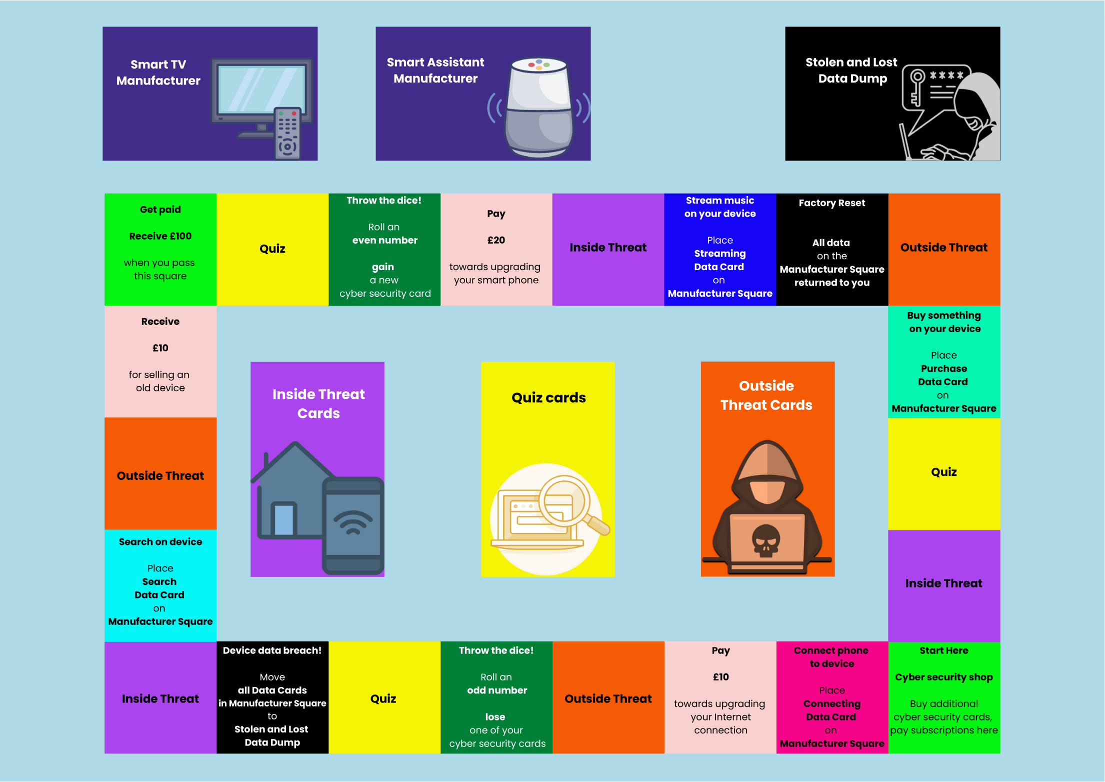

Smart TV Manufacturer
Smart Assistant Manufacturer
Stolen and Lost Data Dump
Get paid Receive £100 when you pass this square
Quiz
Throw the dice! Roll an even number gain a new cyber security card
Pay £20 towards upgrading your smart phone
Inside Threat
Stream music on your device Place Streaming Data Card on Manufacturer Square
Factory Reset All data on the Manufacturer Square returned to you
Outside Threat
Receive £10 for selling an old device
Buy something on your device Place Purchase Data Card on Manufacturer Square
Inside Threat Cards
Quiz cards
Outside Threat Cards
Outside Threat
Quiz
Search on device Place Search Data Card on Manufacturer Square
Inside Threat
Inside Threat
Device data breach! Move all Data Cards in Manufacturer Square to Stolen and Lost Data Dump
Quiz
Throw the dice! Roll an odd number lose one of your cyber security cards
Outside Threat
Pay £10 towards upgrading your internet connection
Connect phone to device Place Connecting Data Card on Manufacturer Square
Start Here Cyber security shop Buy additional cyber security cards, pay subscriptions here

Figure 12: The first game board

was to tie the actions and elements of the gameplay back to the smart TV and smart home assistant. For example, the framing of threat cards was such that it was understandable that they could happen to either a smart TV or smart home assistant. This link was not present in later versions of the game, as will be seen in Chapter 7.

The game board, whilst not in and of itself shaped like a house, or obviously related to a home, allows for players to see the aspects of the game's story unfolding in the squares in the board. For the overall board layout, see Figure 12. Previous research (Jaffray, Finn and Nurse 2021; Chothia et al. 2017) has highlighted the importance of a strong story narrative for immersion within the game: participants here, as the team looking after their smart TV or smart home assistant, are told a story through the cards and activities they encounter.

As detailed out previously in Table 2, there are several potential cyber security measures that could be used in conjunction with the use of home IoT devices to mitigate the types of threats detailed out in Table 1. Cards are vital in conveying this information to participants. The number of cards relating directly to threat types, cyber security measures, and quiz questions remained static throughout the iterations of the game.[10] This is for two reasons: firstly, the number of cards reflected the number of plausibly different scenarios that cyber security could be considered in, as found in news articles and industry reports (for the references that served as inspiration, see Appendix I). As discussed later, the quiz cards allowed for a wider exploration of important topics not easily introduced into scenarios. The idea behind these scenarios and quiz questions was to ensure that participants could directly tie an issue to a potential resolution and then be able to consider the relative importance of the scenario or topic to them, relative to the solution. Table 18 details the links between the scenarios and quiz questions and the solutions that participants could take away from encountering the card. In some cases, the same measure appeared in multiple cards, underlining the relative importance of the measure and the different angles the measure should be considered in (e.g. it is important both to turn on automatic software updates, but it is also important to know how long you can expect to receive those updates on a device). The second, more prosaic, reason for the number of cards was simply to avoid participants cycling through the pack more than once during a gameplay session. Although reiteration of the concepts could be beneficial, knowing that the card had been encountered before could break the participants' engagement with the game.

[10] With one exception, that is discussed later.

Table 18: Scenarios and quiz questions arising in the game linked to the relevant cyber security tools

Card scenario or quiz question	Proposed or discussed cyber security measure
Someone in the house has tried to use your smartphone. Your house is burgled. Your smartphone has been taken. You use your smartphone to connect apps to your device.	Access codes for device applications
Your smartphone has been stolen.	Access code on smart phone
A friend of the youngest member of the family takes too much of an interest in your device. They are too young to understand how to use the device properly and accidentally delete some data.	Back up devices
A malicious hacker decides to scare children by talking to them through devices on insecure networks.	Change router password
Is performing a factory reset enough to delete all your data associated with a device? We have come up with five steps that you should you take before you sell or get rid of a device. Can you name three or more?	Delete device history
Is performing a factory reset enough to delete all your data associated with a device?	Factory reset
One of the children in the house has accessed content you're not happy with on your device.	Family discussion about device use
Someone has decided to play a joke on you by modifying the settings on your device. Someone accesses your email account and password for your device.	Multi-factor authentication
A streaming platform you use on your device has had a data leak, and passwords have been leaked.	Password manager
A relative visits your home, and when looking at your device, presses some buttons, and some settings get deleted.	Profiles for device use
You have a serious falling out with a neighbour who has, in the past, connected to your home Wi-Fi with their laptop and phone.	Review devices on network
How does the UK's National Cyber Security Centre recommend you create strong passwords?	Strong, unique password use
The news reports that a group of cyber criminals have found a vulnerability in your device that enables them to record video and take pictures using the camera.	Tape/cover over cameras
Someone in the house has tried to buy something through your device.	Turn off automatic purchases
You need to do a project at home, that requires talking to lots of people over videochat about quite sensitive things you don't want to be recorded.	Unplug devices when not in use
A friend gives you a USB stick with a game on it. As you plug it in to your laptop, you realise there's a virus on there.	Use antivirus software
You read that your device has a vulnerability that enables people to take a copy of the search histories performed on the devices, if the latest version of the software isn't installed. Can you give two main reasons why apps need updating on devices? How long does a typical smartphone receive automatic software updates ?	Use automatic software updates
Your device has a vulnerability in its software. A cyber criminal tries to access all your devices on the same network, including computers and phones, through this vulnerability. How might you set up your home network to separate your home IoT devices from your smartphones and computers?	Use guest network

Table 19: Card explanations from round one of the game

Card type	How is it incorporated?	Reason for card	Example text
Cyber Security card (see Figure 13)	Teams start play by picking three from the top of the pile	To give teams specific solutions to defend themselves from Inside and Outside Threats Cards may have costs and/or time to set up incurred when teams pick them up: this is to introduce the idea that cyber security measures may not always be free. Cards also provide a "pro" and a "con" about the cyber security measure picked up, to introduce the idea that not all cyber security measures work equally well, or are just beneficial in nature.	Regularly delete device histories : Data collected by devices can typically be deleted, thus making it unavailable to anyone. Cost: None Time to set up: None Pro: The less data a device has, the less there is to be lost, stolen or otherwise used badly Con: The device may often need significant data to offer smart insights or personalisation
Data card (see Figure 14)	Teams start play with two of each type	To embody movement of data from device to manufacturer, and data compromise (by moving to Manufacturer square, and then to Data Exposed Without Your Consent square).	Connecting data: Information you might share when you connect to a device with your smartphone: Your smartphone make, model, software details Your unique device address Other devices on your home network
Outside Threat card (see Figure 15)	Teams pick up a card when they land on an Outside Threat square during gameplay	To provide a scenario of a particular threat, relevant to the team's device, emanating from outside the home. Some of the threats posed on these cards can be mitigated by holding the right Cyber Security card at the time of landing on the square. Without the correct Cyber Security card, the team will be exposed to potential data, time and money loss. Some cards require teams to roll the dice to introduce the concept that sometimes threats do not materialise simply due to chance.	Threat: Your device has been targeted by cyber criminals: if it still uses the default password it came with, it can be used by them to force websites offline. Roll the dice: Odd Number: You changed the password when you set up the device, so it's fine. Even Number: Your Internet Service Provider notices that your device is acting maliciously and bars you from their service. Pay £100 to connect to a new ISP. Move all Connecting Data cards in your Manufacturer square to the Data Exposed Without Your Agreement square.
Inside Threat card (see Figure 16)	Teams pick up a card when they land on an Inside Threat square during gameplay	To provide a scenario of a particular threat, relevant to the team's device, emanating from inside the home. Some of the threats posed on these cards can be mitigated by holding the right Cyber Security card at the time of landing on the square. Without the correct Cyber Security card, the team will be exposed to potential data, time and money loss. Some cards require teams to roll the dice to introduce the concept that sometimes threats do not materialise simply due to chance.	Threat: One of the children in the house has accessed content you're not happy with on your device. If you have the following cyber security card: Family discussion: device use You have a short discussion based on what you've agreed before. If you don't have the card: Skip a turn to discuss ground rules with everyone else.
Quiz card (See Figure 17)	Teams pick up a card when they land on a Quiz square during gameplay	To provide an opportunity to introduce other cyber security concepts that could not otherwise easily be introduced as an Inside or Outside Threat. To provide an opportunity for teams to win money or Cyber Security cards.	Question: How might a ransomware attack on your device's manufacturer affect your device? A) Device may no longer be able to do anything on the Internet. B) You might not be able to access any account information. C) Your personal data may be stolen and given to others without your permission. D) There may not be any effect. E) All of the above are possible. If team answers correctly: Pick a new cyber security card. Answer: E

Having chosen which device they would be, each team starts the game with items that will serve two key purposes: protect them from attack, or be lost as a result of attack or other activity on the board. For an overview of the purpose of the cards in the game, see Table 19. Cyber Security cards and data cards are vital components of the game's story. Although both aspects in the first version of the game are relatively passive, and only used in conjunction with events occurring on the board, they are included to explain more about the role of data, and the role of cyber security measures. Cyber Security cards — chosen at random — are collected by each team and can help protect themselves against threats. For examples of the front side of the card, and various back sides, see Figure 13. Each Cyber Security card would offer a different measure, but potentially at a cost of time to set up, or money (for subscriptions or initial purchase). Cyber Security cards, once gained by a team, could be used to protect against an attack — provided they hold the right card. The teams also start with data cards, and £300 (in play money). To explore the movement of data, and the potential attack vectors being not only the device user, but also the device manufacturer, flows were created in the game that moved data cards from the team to the manufacturer, and possibly then going on to be "exposed without your agreement" (which was a step closer to losing the game altogether). For the data cards from the first round, see Figure 14. Money is used to highlight the ongoing costs of device ownership, whether having to pay bills related to ownership, or for repairs or replacement when activities on the board have negative outcomes.

At this point, it is worth mentioning that the first iteration of the game was unwinnable: as described in the previous paragraph, the goal of the game was to avoid being the first to run out of data or money. As discussed at length in Chapter 7, this was not a design feature that was popular with participants, but was introduced in the first iteration of the game, again, as a reflection on the negative nature of cyber security as a whole: that the risk management aspect of owning home IoT devices typically relies on luck not to lose money or data if you employ no cyber security measures; and if you do employ such measures, they will often come at a time or monetary cost. The researchers and those researchers who participated in the games pilots assumed that there were no natural ways to describe the relationship between the home IoT devices and employing appropriate cyber security measures in a way that could allow for "winning" the game.

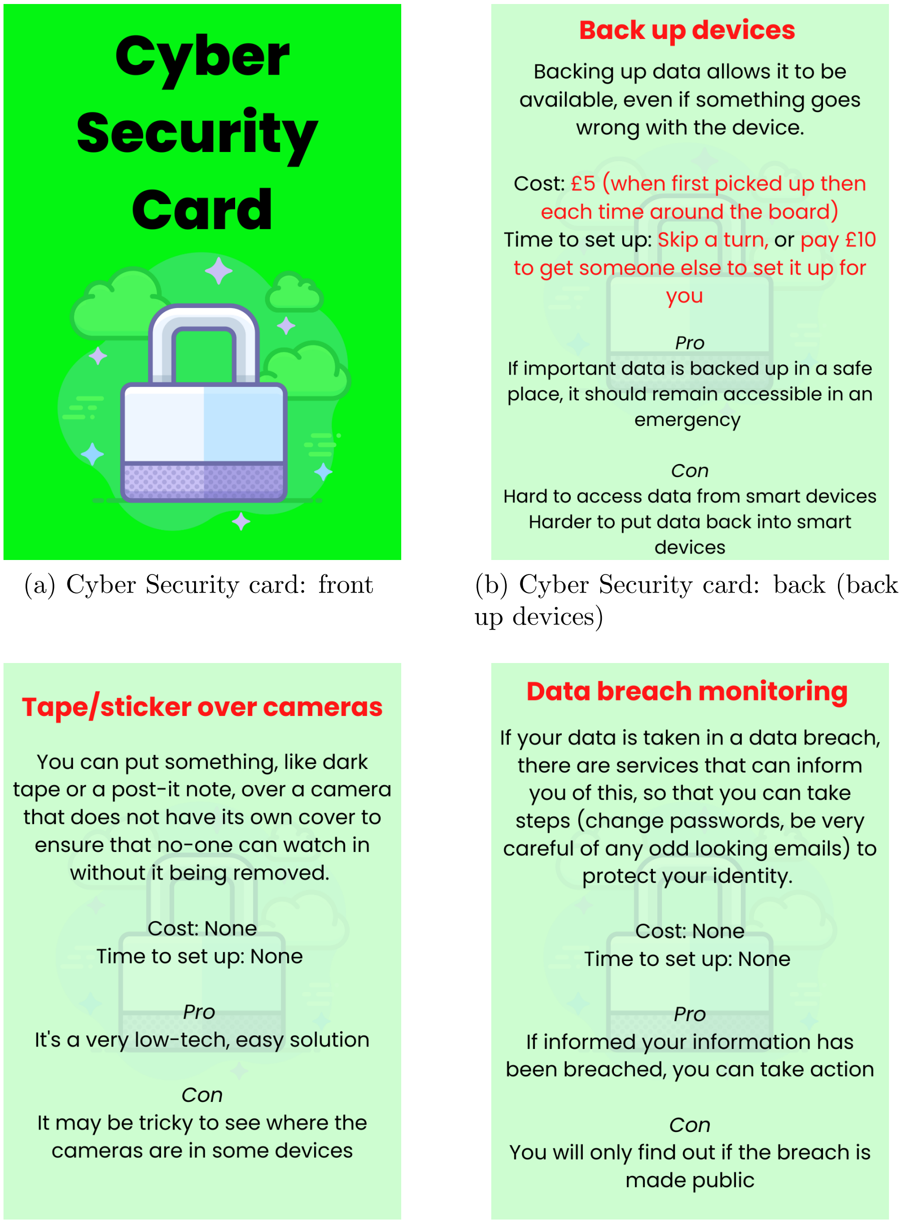
Although, as will be seen, given the feedback in the first round of gameplay, a means of winning the game was introduced in subsequent rounds to increase the enjoyment of the participants.

In order to address *RF 2, 4, 6, 8*, and *9*, significant emphasis is made in the game on the types of threats that can be posed by home IoT that may not be familiar to participants used to thinking about using the Internet on a computer. Furthermore, due to a prevalence of answers in the interviews and surveys in Chapter 4, and the framing of the majority of threat actors in advice articles in Chapter 5.2 such that the only threats that could be posed would be by hackers or nation states, rather than considering the more mundane and probably likely, it was decided that threats should be split into two categories. *"Outside Threats"* would indeed cover acts of cyber crime and damage that are faceless and, often, not targeted directly at the home IoT device user. For examples of the front and backs of Outside Threat cards used in round one, see Figure 15. *"Inside Threats"*, conversely, would aim to bring to light the threats to device use that may be much closer to home — the types of threat that would be much more likely to happen, but seemingly discounted by interview and survey participants as not relevant or important. The game attempts to make the case that whilst outside threats can be dangerous, inside threats can be just as catastrophic in terms of data loss and device damage — but they are just not perpetrated by those with criminal intent; much more likely, they will be accidental in nature, but the outcome remains the same. For examples of the front and backs of Inside Threat cards used in round one, see Figure 16.

In order to make the threats more vivid and engaging, they were incorporated into short scenarios, using language to suggest that the team who had landed on the relevant square had suffered the attack. Following research such as Pfeffer et al. (2022), the intention was to use the storytelling aspect of the scenario, and the immediate retelling of the scenario to all gameplaying participants, as a way of reinforcing the potential damage that the threat being considered could create. Additional reinforcement of the consequences of the threat would be felt immediately: either the team would be able to protect themselves through having the correct cyber security measure, or they would lose some combination of data and/or money.

More general learning about cyber security measures that could not be incorporated into threat scenarios were included in Quiz cards (see Figure 17). These cards offered the opportunity for direct learning on specific topics, addressing *RFs 3, 8 and 10*, but, in terms of the game story, allowed for the ability to win Cyber Security cards, or money. Rewarding correct answers reinforced the value of understanding the concepts being discussed, although wrong answers also provide opportunities for discussion and learning.

Table 20 gives an overview of the squares on the board and the actions that landing on the square could lead to. To see the board in its totality, see Figure 12.



Cyber Security Card

(a) Cyber Security card: front

Back up devices

Backing up data allows it to be available, even if something goes wrong with the device.

Cost: £5 (when first picked up then each time around the board)
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
If important data is backed up in a safe place, it should remain accessible in an emergency

Con
Hard to access data from smart devices
Harder to put data back into smart devices

(b) Cyber Security card: back (back up devices)

Tape/sticker over cameras

You can put something, like dark tape or a post-it note, over a camera that does not have its own cover to ensure that no-one can watch in without it being removed.

Cost: None
Time to set up: None

Pro
It's a very low-tech, easy solution

Con
It may be tricky to see where the cameras are in some devices

(c) Cyber Security card: back (tape over cameras

Data breach monitoring

If your data is taken in a data breach, there are services that can inform you of this, so that you can take steps (change passwords, be very careful of any odd looking emails) to protect your identity.

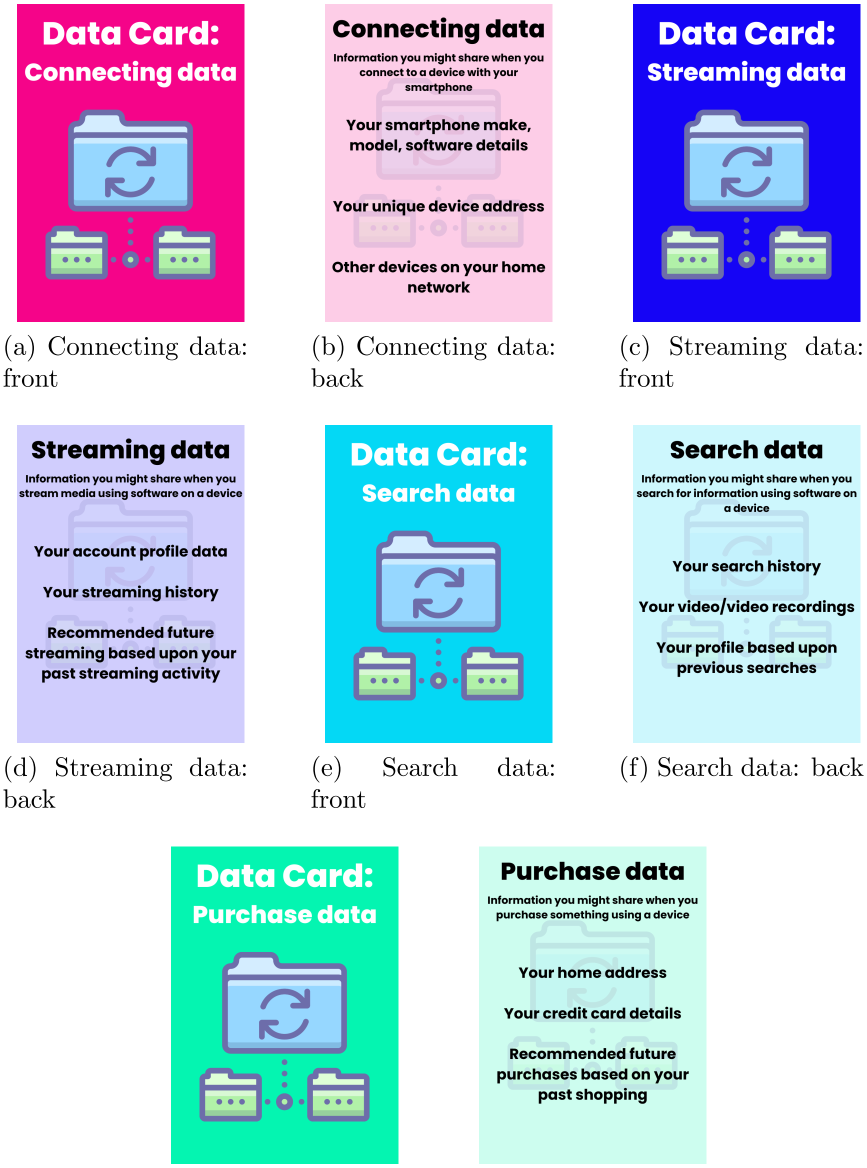
Cost: None
Time to set up: None

Pro
If informed your information has been breached, you can take action

Con
You will only find out if the breach is made public

(d) Cyber Security card: back (data breach monitoring)

Figure 13: Round one: Cyber Security cards



Data Card:
Connecting data

(a) Connecting data: front

Connecting data

Information you might share when you connect to a device with your smartphone

Your smartphone make, model, software details

Your unique device address

Other devices on your home network

(b) Connecting data: back

Data Card:
Streaming data

(c) Streaming data: front

Streaming data

Information you might share when you stream media using software on a device

Your account profile data

Your streaming history

Recommended future streaming based upon your past streaming activity

(d) Streaming data: back

Data Card:
Search data

(e) Search data: front

Search data

Information you might share when you search for information using software on a device

Your search history

Your video/video recordings

Your profile based upon previous searches

(f) Search data: back

Data Card:
Purchase data

(g) Purchase data: front

Purchase data

Information you might share when you purchase something using a device

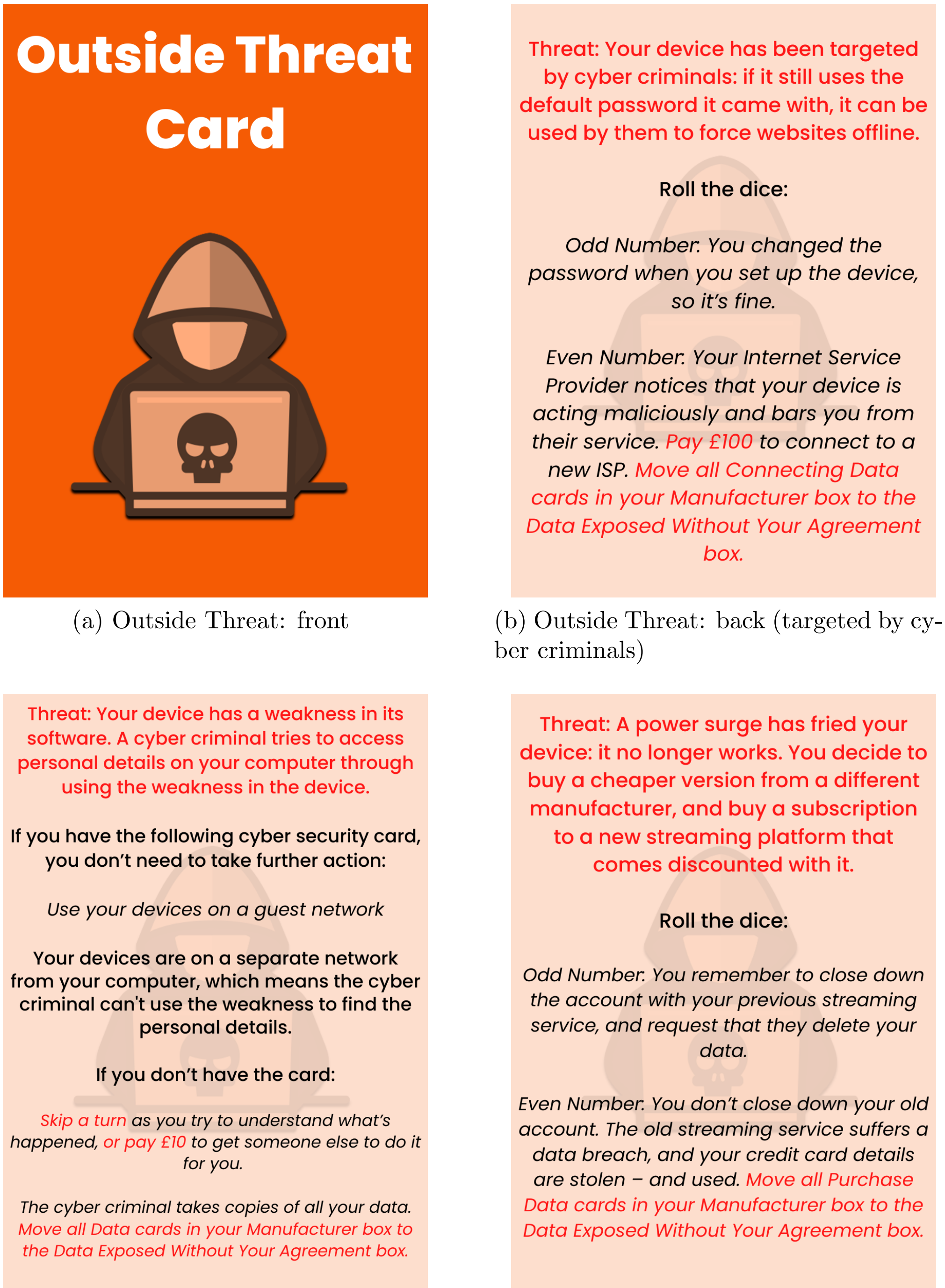
Your home address

Your credit card details

Recommended future purchases based on your past shopping

(h) Purchase data: back

Figure 14: Round one: Data cards



Outside Threat Card

(a) Outside Threat: front

Threat: Your device has been targeted by cyber criminals: if it still uses the default password it came with, it can be used by them to force websites offline.

Roll the dice:

Odd Number. You changed the password when you set up the device, so it's fine.

Even Number. Your Internet Service Provider notices that your device is acting maliciously and bars you from their service. Pay £100 to connect to a new ISP. Move all Connecting Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

(b) Outside Threat: back (targeted by cyber criminals)

Threat: Your device has a weakness in its software. A cyber criminal tries to access personal details on your computer through using the weakness in the device.

If you have the following cyber security card, you don't need to take further action:

Use your devices on a guest network

Your devices are on a separate network from your computer, which means the cyber criminal can't use the weakness to find the personal details.

If you don't have the card:

Skip a turn as you try to understand what's happened, or pay £10 to get someone else to do it for you.

The cyber criminal takes copies of all your data. Move all Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

(c) Outside Threat: back (weakness in software)

Threat: A power surge has fried your device: it no longer works. You decide to buy a cheaper version from a different manufacturer, and buy a subscription to a new streaming platform that comes discounted with it.

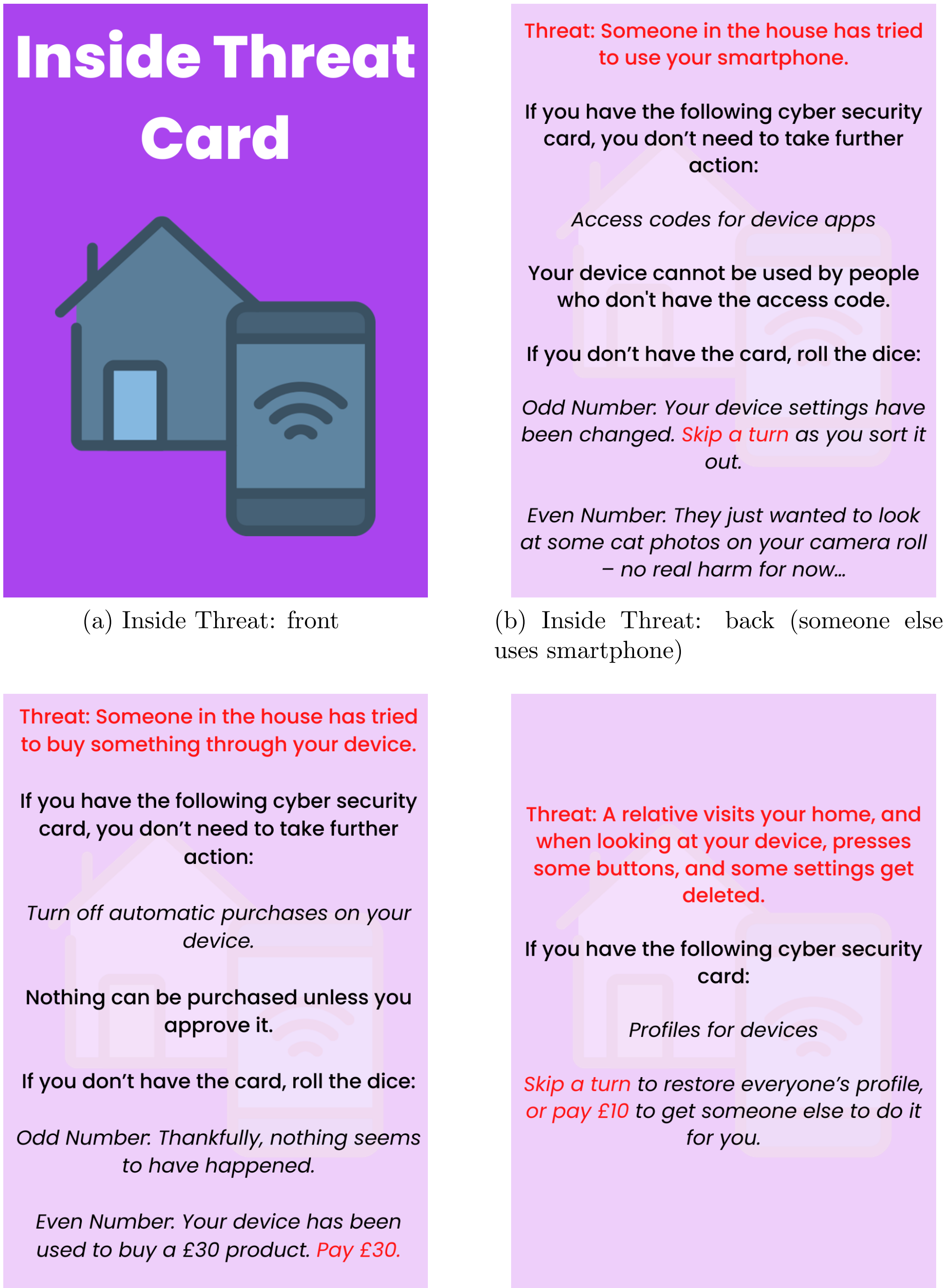
Roll the dice:

Odd Number. You remember to close down the account with your previous streaming service, and request that they delete your data.

Even Number. You don't close down your old account. The old streaming service suffers a data breach, and your credit card details are stolen – and used. Move all Purchase Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

(d) Outside Threat: back (power surge)

Figure 15: Round one: Outside Threat cards



Inside Threat Card

(a) Inside Threat: front

Threat: Someone in the house has tried to use your smartphone.

If you have the following cyber security card, you don't need to take further action:

Access codes for device apps

Your device cannot be used by people who don't have the access code.

If you don't have the card, roll the dice:

Odd Number. Your device settings have been changed. Skip a turn as you sort it out.

Even Number. They just wanted to look at some cat photos on your camera roll – no real harm for now...

(b) Inside Threat: back (someone else uses smartphone)

Threat: Someone in the house has tried to buy something through your device.

If you have the following cyber security card, you don't need to take further action:

Turn off automatic purchases on your device.

Nothing can be purchased unless you approve it.

If you don't have the card, roll the dice:

Odd Number. Thankfully, nothing seems to have happened.

Even Number. Your device has been used to buy a £30 product. Pay £30.

(c) Inside Threat: back (unauthorised purchase)

Threat: A relative visits your home, and when looking at your device, presses some buttons, and some settings get deleted.

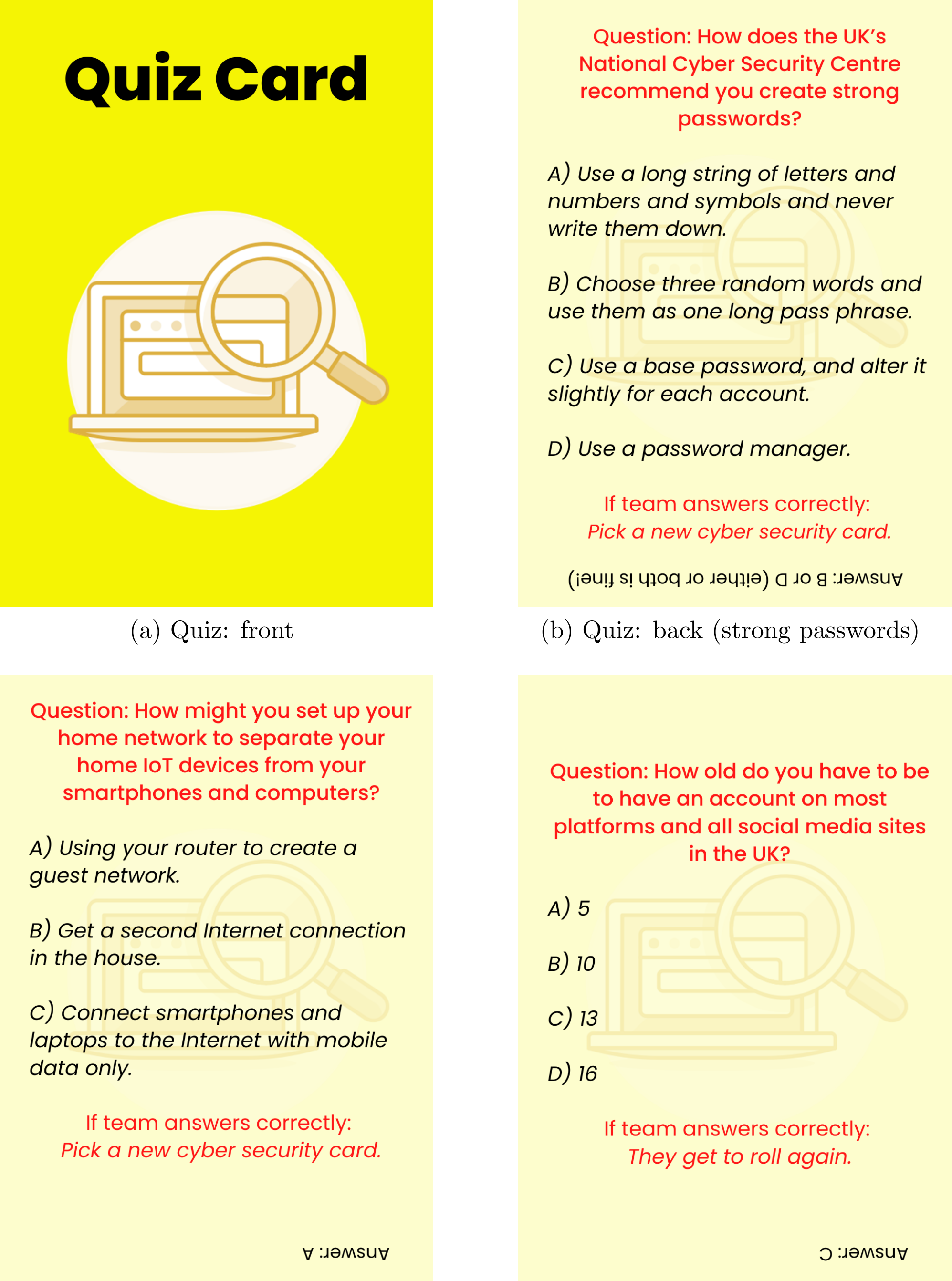
If you have the following cyber security card:

Profiles for devices

Skip a turn to restore everyone's profile, or pay £10 to get someone else to do it for you.

(d) Inside Threat: back (deleted settings)

Figure 16: Round one: Outside Threat cards



Quiz Card

(a) Quiz: front

Question: How does the UK's National Cyber Security Centre recommend you create strong passwords?

A) Use a long string of letters and numbers and symbols and never write them down.

B) Choose three random words and use them as one long pass phrase.

C) Use a base password, and alter it slightly for each account.

D) Use a password manager.

If team answers correctly:
Pick a new cyber security card.

Answer: B or D (either or both is fine!)

(b) Quiz: back (strong passwords)

Question: How might you set up your home network to separate your home IoT devices from your smartphones and computers?

A) Using your router to create a guest network.

B) Get a second Internet connection in the house.

C) Connect smartphones and laptops to the Internet with mobile data only.

If team answers correctly:
Pick a new cyber security card.

Answer: A

(c) Quiz: back (guest network)

Question: How old do you have to be to have an account on most platforms and all social media sites in the UK?

A) 5

B) 10

C) 13

D) 16

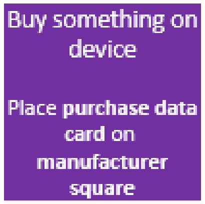
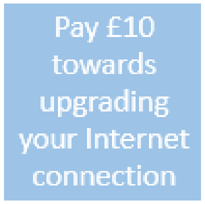
If team answers correctly:
They get to roll again.

Answer: C

(d) Quiz: back (social media)

Figure 17: Round one: Quiz cards

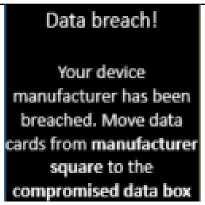
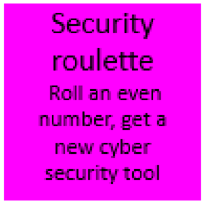
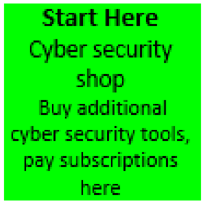
Table 20: Squares and actions from round one of the game

Type of square	Example	Explanation
Device Action	 Buy something on device Place purchase data card on manufacturer square	Participants have to hand over a data card “to the manufacturer” (a separate box on the board) for doing a standard activity with a device (connecting a smart phone to the device, buying something on the device) — the intention behind such squares is to link the use of devices in different ways with different types of data transfers.
Pay/Receive Money	 Pay £10 towards upgrading your Internet connection	These squares link costs to home IoT device usage (upgrading Internet connection or upgrading a smart phone), and also allow for teams to gain money by “selling an old device”. Similarly, there is the “Get Paid” square, which facilitates ongoing gameplay by giving participants an extra £100 each time they pass it.

Continued on next page

Type of square	Example	Explanation
Outside/Inside Threat	Inside threat	These squares require the team to face a scenario based upon an Outside or Inside Threat (that is, a threat that is either posed from outside of the people or devices within the home, or a threat posed by people or situations occurring within the home). The team that lands on the square then has to deal with the consequences of the threat that has occurred. Consequences may be mitigated by owning specific cyber security tools, or through a throw of the dice. The dice throw is used to recognise the fact that practicing poor cyber security, for example, does not always mean a poor outcome, and that this survivorship bias, or chance, may account for a significant percentage of cyber security decisions by individuals.
Quiz	Quiz	These cards pose general cyber security questions to the team that lands on the square, with the opportunity to win in game prizes for correct answers.

Continued on next page

Type of square	Example	Explanation
Data	 Data breach! Your device manufacturer has been breached. Move data cards from **manufacturer square** to the **compromised data box**	There are two of these squares, one invoking a data breach, the other a factory reset — providing the opportunity for the team either to lose data permanently (a step closer to losing the game), or regain all the data they had previously provided to manufacturers by connecting to devices.
Security Roulette	 Security roulette Roll an even number, get a new cyber security tool	These squares give the team that lands on them the opportunity to gain, or lose, a cyber security tool.
Shop/Get Paid	 **Start Here** Cyber security shop Buy additional cyber security tools, pay subscriptions here	These squares facilitate elements of gameplay. Aside from being the starting point of the game, the “Start Here” or “Cyber Security Shop” tool allows for the collection of subscriptions or purchase of new tools; the “Get Paid” square gives teams £100 when they pass, to ensure teams do not run out of money too quickly within the game.

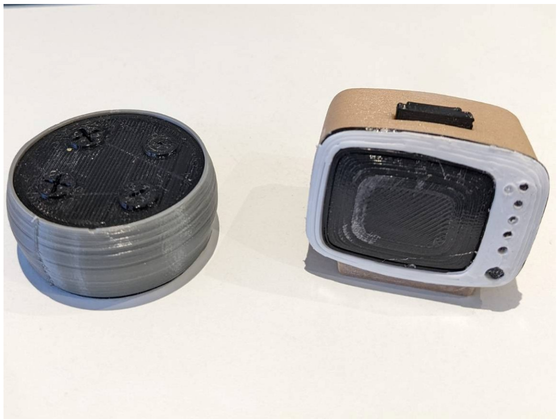


Figure 18: 3D printed game counters

6.3.3 Technology and Aesthetics

The concepts of Technology and Aesthetics from Schell's *elemental tetrad* will be considered together here, as aspects of the physical pieces and how they were presented are clearly linked, particularly given the obvious prototype nature of the design in the first round. As such, aesthetics in particular were designed at a low level with a specific desire to get suggestions for improvements from participants.

Once the decision was taken, for the reasons described above, to use the board game format, there were implications on the subsequent "technologies" that would be used, namely, that there would need to be cards and game pieces to facilitate the gameplay. Barring a complete redesign of the game, the combination of board, cards, game pieces would remain as the key pieces of technology in the game.

In order to create a game board that could enable gameplay without significant design time or costs, the initial board design was created in PowerPoint, and printed on to an A2 sheet of foam-board. This allowed for clarity of squares, and basic aspects of continued design (aesthetic) features, such as consistent colour use for squares and linked cards, as well as the introduction of graphics to represent the Threats and Quiz. Although somewhat rudimentary in approach, the consistency was considered important to allow for players to start to have an immersive game experience by not having to do the mental heavy lifting of linking the square that they had landed on to the action they subsequently needed to take.

The cards needed for gameplay — the Threat, Quiz, Data and Cyber Security cards — were printed, in colour and double-sided, on A7 card. A7 was chosen, despite being, arguably, bigger than average playing cards, to provide sufficient space for scenarios and questions in a large enough font. Key phrases, words and actions, were highlighted in red for additional ease of reading. The use of card (instead of paper), along with the professional print finish of both the cards and the board, provided the start of a feel of the quality of a real board game that Hart et al. (2020) had pointed out was vital to draw players into the game. Custom-made 3D printed game counters added to this idea of being more than a prototype (see Figure 18). All round one game cards are detailed out (one copy of the front of each type of card, followed by each back side) in Appendix H.

6.3.4 Initial game summary

This chapter has recounted the explanation behind and setup of the final piece of research in this thesis, which addresses RQ4 — how can a board game act as an intervention to support participant families to improve awareness in relation to the cyber security of home IoT devices that they own and use? This chapter has explained the starting point of the research with family participants, both in terms of the methodology of the process, but also in terms of the decisions made behind the creation of the first round of the game. The board game for round one had been built in part to address findings from the previous pieces of research in the thesis, and with the knowledge that, coming from a place of lack of awareness, families needed an interactive form of training and education to move from a place of precontemplation. These aspects were combined with examples and guidance from real-world sources to create a number of activities that came together to create a game for two teams, incorporating ideas that could translate into learning about different threat types, more general cyber security knowledge, and the nuance of whether cyber security measures were relevant or useful. It also, in giving teams data to protect as well as money, tried to show players that not all that they should be concerned about is monetary loss. Game rules were created to facilitate game setup and explanations as to how to perform the actions assigned to squares, as they were landed on. The version presented to family participants was the result of two rounds of pilot tests within the university department: these sessions provided changes to improve clarity, rather than gameplay changes. Chapter 7 will go on to give details of the results of the UCD effort, and look at whether the game could be said to serve as a cyber security intervention for families.

Chapter 7

The creation of an intervention to promote positive cyber security actions amongst families: findings

Following on from the explanatory work of the previous chapter, this chapter will explore the findings from the gameplaying sessions. For ease of understanding, the findings will be addressed in two parts. First: the findings from the UCD of the game, from the first version, described in Chapter 6.3, to the version played with in round three will be presented round by round. Second: the value of the serious game will be considered: did the game make participants more aware of the threats and risks of using home IoT devices, and did participants make changes in their cyber security setup at home?

This is presented as follows. Section 7.1 walks through the findings from the three rounds of gameplaying sessions, first in terms of the UCD process (and the development of the game based upon the feedback from each round), then in terms of the cyber security findings. The findings are discussed in Section 7.2, with more of an expanded discussion section than previous chapters, as well as an overview of the *RFs* generated from the research. Finally, Section 7.4 summarises the process and findings from the chapter, and some of the implications arising from the discussion.

7.1 Findings from gameplay

This section will be broken down in two parts, in line with the two key purposes of the gameplay sessions: a) the creation of a more enjoyable, more engaging game by the point of playing in round three, and b) the value of the game in improving cyber security discussions and awareness in the families that played it. The findings relating to the UCD process are extremely important, despite being slightly separate to the goal of researching cyber security. With the cyber security material (i.e. the quiz questions, the threats, the cyber security measures) within the game remaining almost identical throughout (except where detailed below), the relevance of the UCD process can be seen in whether the post-gameplay outcomes improved, round upon round. This would show that the medium of knowledge transfer — namely, the version of the game being played — was important in affecting the results.

In both sections, the participant families will be referred to in the following way: the round number, followed by the family code (as listed in Table 16: L referring to families that participated in London, K in Kent, and O online). Adults will be referred to as AF or AM, based upon whether they were female or male, and children will be referred to as C1, C2, C3 or C4 (descending in age), with their age after. That is to say, the male adult participating in round one, from Family K1 will be referred to as R1K1AM; the second-eldest child in the same family will be referred to as R1K1C2, aged 13.

7.1.1 User-centred design findings

The findings explored below are based upon three elements of the gameplaying process: the gameplay itself, the interview immediately following the gameplay, and the free text field asking for further feedback in the survey undertaken a week after gameplay. As mentioned above, for ease of narrative, the following sections will be considered chronologically: that is to say, the findings of round one will be discussed, and the version of the game taken into round two will be explained before moving into the findings for round two, and so on. After that, there will be a brief discussion of the enjoyment ratings provided in the final survey, and some discussion of the implications of the UCD aspect of the game.

7.1.2 Round one feedback

The game taken into round one has been explained in depth in Chapter 6. As such, no further explanation of the game will be provided here. The flow of these findings will be split up in the following way: an overview of likes, dislikes and confusions arising from the first round of gameplay will be considered, followed by specific aspects of improvements that participants suggested. This will be accompanied by an overview of the precise changes made to the game between rounds one and two, before an introduction of the second version of the game.

The process behind making improvements

As is the case with any piece of work created through UCD, the generation of ideas are — hopefully — sufficient in number and quality that some are not taken forward. This was the case for round one. In addition, improvements also became evident to the researcher, having watched families struggle with certain aspects of the gameplay repeatedly. After the first round of gameplaying was completed, the merits of improvements suggested, and those noted as likely necessary to improve gameplay, were considered in relation to the following factors:

- **Obviously difficult or confusing gameplay:** Where the researcher noted the majority, or all, of the families struggling with certain aspects of the gameplay changes were considered. These problems also had suggestions made by the families too, and so the changes were informed by both participant suggestion and the need seen by the researcher (e.g., the removal of the data flow process).

- **Strength of feedback:** numbers of families suggesting there was a problem or improvement to be made in gameplay around a specific aspect or piece of design (e.g., changing the game to allow for a clear winner).

- **Adherence to good cyber security and cyber hygiene:** suggestions that could lead to participants gaining incorrect understandings about good cyber security were not taken forward (e.g., suggestions around selling data to gain money).

- **Including the possible:** some suggested improvements involved redesigning the game to an extent not possible to incorporate (e.g., the inclusion of smart home assistants to ask questions).

- **Include items that improve the specific learning experience:** suggestions that had the potential to reduce some of the learning experience (e.g., removing money or data in gameplay entirely) were not taken forward. However, all suggestions that improved the clarity of gameplay or the engagement of gameplay (e.g., reducing the amount of text, altering the game to allow for winning) were taken forward.

- **Elements of gameplay that altered focus from the target audience:** Feedback that suggested the inclusion of elements for other target groups, rather than secondary school children and their parents, was not incorporated to avoid scope creep (e.g., the idea of making the game more generic to be played in several settings).

As will be seen in the evolution of the game, in a couple of cases, changes were suggested and taken through on the basis of the steps above, only for the next round of families to suggest that they did not like the changes made. This was particularly the case for the amount of text on the cards, where a reduction in the amount of text came at a cost of losing background information (that was provided in the accompanying booklet, but not on the cards itself); the size and layout of the board similarly took all three rounds to get to a version that was appreciated by the majority.

Likes, dislikes and confusions

Likes:

Despite the fact the game was in an early stage of creation for round one, participants could still point to areas of enjoyment, or things that they liked. In the main, these were aspects that would come out in later stages as well, and perhaps in more muted tones than in later stages, particularly in the written feedback. **The ability to start a family conversation** was noted — *"...this is a good way to communicate with younger ones, like C2, aged 10; [the ideas covered in the game] can be a bit abstract"* (R1L7AF). Children too expressed how they would like to play the game in school and further at home, giving more opportunities to continue learning from the game: *"Can I take it home?"*

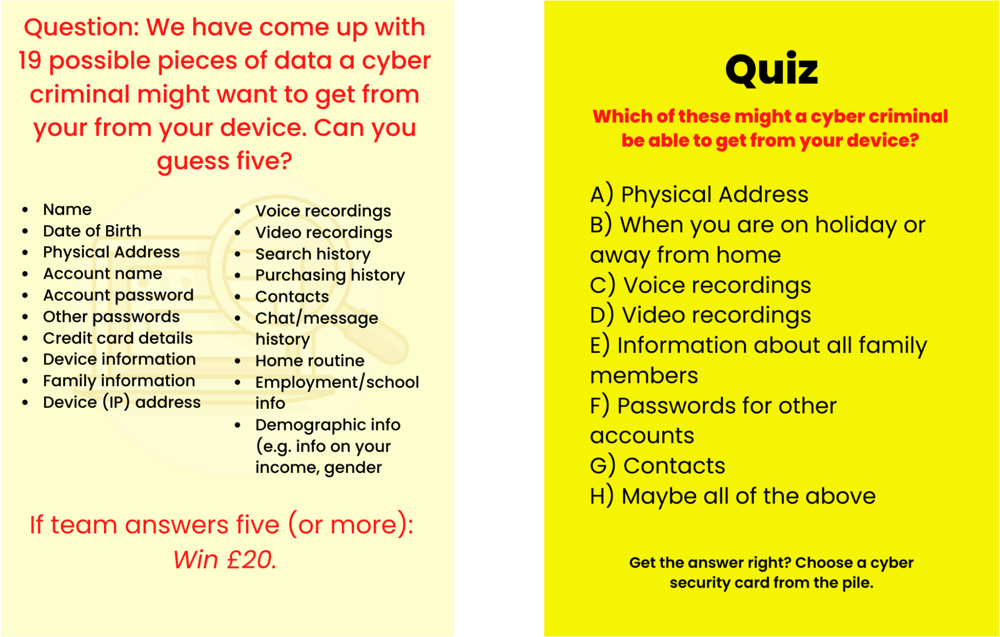
(R1L5C2, aged 8); *"We could use this in lessons!"* (R1K3C1, aged 12). This may have been in part because of the **look of the game** — adult participants suggested that it could be enticing to younger children because of the range of colours and symbols used, even if the application at this point was clearly quite basic. *"I really liked [the cards] because they have pictures and symbols. That means you can recognise them quite quickly"* (R1K3AF). That said, participants also pointed out the potentially exclusionary element of an unconsidered approach to using multiple colours: *"Colour blind people cannot necessarily read words against specific colours — and some fonts are better than others"* (R1K1AM).

The Quiz cards were by far and away the most enjoyed element of the game: *"You know, I love the Quiz"* (R1L9A1). Many families reflected that that was because of the **element of competition** that they introduced; they also allowed for interaction between teams. As a result of the random nature of gameplay, Family R1K1 did not encounter the Quiz component until quite late on in their playing. R1K1AF reflected that *"if we'd have had a few more quizzes, then we would have had more interaction: 'oh my gosh, the thing that's the answer...[and] I don't know the answer to that' — that kind of thing"*.

Dislikes and confusions:

By far the biggest disappointment for many families — stemming directly from the enjoyment of the competitive aspect mentioned above — was the fact that **the game was unwinnable**. *"This game is about not losing your data. So it's quite the opposite [of winning something]"* (R1L2AM). The lack of a positive goal to work towards was quite a mind shift from other board games: *"...often at the start of the game, you know there's a goal. Ironically [with this game] you're already at the goal already and the goal is being slowly taken away."* (R1L3AF). R1K1C3, aged 9, summed it up, when asked what he liked about playing board games: *"Winning!"*

In addition to not being able to win, participants agreed that there was **too much text on the cards** — for example, survey feedback from Family R1L2: *"it was a little wordy..."*; *"We had quite a lot to read on the cards, and the kids are not a fan of reading..."* (R1K5AF). Younger children, when asked to read out threat scenarios or Quiz questions, sometimes struggled to read the entire scenario, and occasionally would trip over more technical language (for example, "authenticator" or "ransomware"). Quiz questions, too, whilst generally extremely popular, also caused problems in instances where the questions were phrased in such a way that participants were asked to list things out (such as the one shown in Figure 19a). This proved complicated, and also created situations where the team being asked would provide an answer in slightly different wording than that provided on the card, leading to further confusion. *"[The Quiz cards] you had to guess...some of those were really hard"'* (R1L6C1, aged 12).



Question: We have come up with 19 possible pieces of data a cyber criminal might want to get from your from your device. Can you guess five?

- Name
- Date of Birth
- Physical Address
- Account name
- Account password
- Other passwords
- Credit card details
- Device information
- Family information
- Device (IP) address
- Voice recordings
- Video recordings
- Search history
- Purchasing history
- Contacts
- Chat/message history
- Home routine
- Employment/school info
- Demographic info (e.g. info on your income, gender

If team answers five (or more): *Win £20.*

Quiz

Which of these might a cyber criminal be able to get from your device?

A) Physical Address
B) When you are on holiday or away from home
C) Voice recordings
D) Video recordings
E) Information about all family members
F) Passwords for other accounts
G) Contacts
H) Maybe all of the above

Get the answer right? Choose a cyber security card from the pile.

(a) Round one: listing out

(b) Subsequent rounds: multiple choice

Figure 19: Quiz question: change from requiring participant to list out answers to multiple choice

The **complexity of certain aspects of the game process** also felt difficult and confusing to the participants. One aspect in particular stood out: teams could lose data cards in one of two ways. This process was included to try and elicit the understanding that data could be "exposed without your agreement" (the game's terminology for having data breached and potentially abused) at multiple points in its existence. In particular, for the game, data could be exposed directly (by someone stealing a smartphone, for example) or indirectly, through attacking the device manufacturer. This was represented in the game by having scenarios where data cards would be moved directly to the "data exposed without your agreement" box; in other instances, the team would "connect their device" to carry out particular functions (streaming or purchasing, for example). This would result in data cards being moved to the "manufacturer". This data would then be vulnerable to attack from Outside Threat cards, in particular, where adversaries could attack the data storage of the manufacturer. In that case, the data held by the manufacturer would be moved to the "data lost without your agreement" square. It was generally agreed that trying to express this multistep relationship was too complex to understand in the gameplay: *"It was a bit tricky with some of the cards moving from place to place"* (R1L5AF); *"...it was a bit difficult to get my head around"* (R1L9C1, aged 18).

The lack of understanding around that element of gameplay was compounded by the difficulties that were felt around **understanding what the data cards were**. Families — especially children — could instinctively understand the value of the play money that they had *"I liked the money!"* (R1L8C3, aged 9), *"I enjoyed playing with the money"* (R1K3C2, aged 10). In fact, the focus on money instead of data was so prevalent that participants sometimes suggested actions to gain more at the expense of protecting their data: *"Maybe you could sell that data, so you could get more money?"* (R1L10C1, aged 14). The same level of ownership, and desire not to lose them, was not felt over the Data cards. R1K3AF summed up the issue like this: *"The [Data cards] seemed like property. And quite honestly, if I don't feel like I own the property in the first place, I don't really care if it's gone somewhere."*

It should be noted, as something seen throughout all rounds, that a number of families recognised that it would have been beneficial **to be able to play the game more than once**. Again, R1K3AF explained this most clearly of all participants:

> *We knew it was only half an hour, so we wanted to speed through the game. So we didn't take too much time on reading the information. I think if it was a game that we had at home, we probably all would have played a game like that. But probably then read it all afterwards, and then probably played it again, and again.*

Improvements suggested

This section will be broken down into two main areas: suggestions arising from families about how to change or improve the gameplay, and more specific aspects of the design of the board, cards and pieces. Some of these aspects flow naturally from the dislikes and confusions arising in the game.

Gameplay

Make the game more positive:

As mentioned in the previous section, participants wanted to be able to **play to win**, requiring an alteration of the core gameplay of the game. Several families thought that this could be achieved, in part, through shifting the focus to **collecting things**, whether it be starting the game with no Cyber Security cards and building up your security portfolio over time, or, as one participant suggested, *"maybe there's a shield representing your knowledge growing and showing how your defences are getting better. So you might only get 90%, but the other team will have 10%, and if you've lost all your cards, at least you've gained more knowledge than them!"* (R1L7AM). This would put a more positive spin on what could be seen as the inherently negative process of avoiding losing data and money.

Improvement 1: Make the game winnable.
Improvement 2: Focus on collecting things (possibly knowledge).

Mix up gameplay:

The Quiz was by far the most engaging aspect of the game. This prompted participants to reflect upon what could not only make the game more engaging, but how aspects of the game could become more integrated. One family reflected upon how much they had enjoyed it when their opposing team had lost Quiz questions, and how that sentiment should be carried over to make a game where you cared more about **sabotaging the other team** rather than simply considering your own progress. *"Could you have it that we're basically working against each other...that we're the threat against each other?"*(R1K3C1, aged 12). In addition to this was an interest in expanding out the range of devices, from just the smart TV and smart home assistant, to make them a more interesting feature in the game — *"I would have more devices..."* (R1K1C1, aged 14), *"You could have a little laptop or game console?"* (R1K5AF), *"Because the devices don't mean anything...I would have [more, like] a Playstation, laptops, Alexas, smartphones, TVs..."* (R1L10C1, aged 14).

Improvement 3: Improve interaction by adding adversarial play.
Improvement 4: Increase range of devices in gameplay.

Design Features

Board:

As makes sense for the stage of development of the game, participants thought more could be made of the design of the board. This was particularly the case with participants with professional graphic design experience. R1L7AM, for example, made significant suggestions about the value having more considered graphics might have both on the layout of the board, but also in terms of making the "data exposed without your agreement" square scarier:

> *...from an illustrative point of view, I think you could make it a lot more fun. You're starting to do stuff here. But, you know, rather than clip art based stuff...That's fine as placeholders to get everything obviously, you know, this journey could feel a bit more of a...less of a go around in circles kind of thing. [You could] just visualize what the darkness [of the "data exposed without your agreement" square] is...less of a person, it could be just like nasties or teeth...*

Other participants thought that there could be a more interesting layout of the board squares, such as *"a snake"* (R1K5AF, and a better use of space on the board. Family R1K3, for example, suggested that the board felt a bit *"squashed"*, and that perhaps it might make sense to add things like the bank and other cards around the board *"like a pattern"*.

Improvement 5: Improve graphics used on the board.
Improvement 6: Board layout improvements.

Cards and Pieces:

As mentioned above, participants wanted **cards to have fewer words**, and be more accessible by linking colours and pictures together. Watching the gameplay also presented two further elements that did not work as expected: **teams did not follow the requirement to pay for Cyber Security cards, either a one-off payment or a subscription payment** (due each time they finished a lap of the board), **or, skip a turn to set up the devices**. These elements were supposed to highlight the trade-offs inherent in choosing cyber security measures — that there is often a cost or time to set up incurred. A further complexity arose in all Cyber Security cards having different levels of payment or skipping a turn (with some having neither). Participants forgot to impose paying, both in the case of one-off payments or subscriptions. In one case, a player immediately realised that the best thing to do would be to chose Cyber Security cards that allowed you to skip a turn, to avoid inevitable loss of data or money:

> R1K3C2, aged 10: *These cards were really good because you get to skip a turn.*
> R1K3AF: *It's tactical, isn't it?*

Watching gameplay also allowed for two further realisations: firstly, the realisation that some cyber security measures were consistently misunderstood. In particular, this was the case for "data breach monitoring", which participants typically assumed was the action of receiving an email from a data controller post-breach (as opposed to signing up with services like Have I Been Pwned[1]). Given the confusion that subsequent discussion between researcher and participants had when discussing this measure, the decision was taken to remove that card.

Secondly, the researcher had the realisation that **having various types of prizes for winning a Quiz or Threat card was imposing too much of a cognitive load on the participants**, and slowing down gameplay (as each time they had to ensure they had won the correct prize). Standardisation, as much as possible, would be a way to reduce time spent considering what a team had just won. Finally, as mentioned above, **the complexity of some of the Quiz questions made them too hard to answer**. This was the case in which the

[1] `https://www.haveibeenpwned.com/`

team being asked the question had to list off things in order to answer the question (e.g., types of personal data).

The **data cards were also an element in need of significant improvement**. As mentioned above, participants struggled to conceptualise what the data cards were, and that they were supposed to have a value akin to the money they were also losing. Several participants suggested altering the shape of the data, to stop them looking more like the other cards in the game. Family R1K5 suggested data could be represented with something else, perhaps *"like a little chip or like a little SIM card"*. R1L2AF suggested the idea of tokens: *"I feel like I almost feel like you need to have like a token or something. I know it's not a physical....something representing that data that you feel like...like chips or something."*

Improvement 7: Reduce words, improve clarity of cards.

Improvement 8: Simplify cards to remove actions that were ignored in the gameplay.

Improvement 9: Standardise prizes won.

Improvement 10: Make Quiz questions have closed-ended answers.

Improvement 11: Alter the appearance and role of the data cards.

7.1.3 Game changes: round two

As described in Table 21, a number of changes were made to almost every aspect of the game following the completion of the first round. These changes will now be detailed out below, before reviewing the feedback of participating families in round two.

Gameplay

In keeping with **Improvements 1 and 2**, the largest shift in the game between round one and two was that of changing it from a game that could not be won, to one that could. Both Improvements 1 and 2 worked together, as suggested by the participants in round one, to produce a game that allowed players to create a sense of collecting things, as well as being able to come to a final, defining point of winning.

The aspect of collection, in fact, became a core aspect of winning the game.

Table 21: Full list of game improvements

Round	Improvment number	Suggested Improvement	Improvement Made
1	1	Make the game winnable.	The fundamental gameplay altered to allow teams to win the game.
1	2	Focus on collecting things (possibly knowledge?)	The concept of collecting knowledge was introduced, by way of collecting wedges in a shield, as part of the altered gameplay to allow for winning.
1	3	Improve interaction by adding adversarial play.	The role of Inside Threat cards changed so that a team landing on the Inside Threat square would be attacked by the other team. Cyber Security Battles introduced to allow for more interactions between teams.
1	4	Increase range of devices in gameplay.	Teams no longer the "smart TV" or "smart home assistant" team. Rather, each team has three devices during the game that they must protect using their Cyber Security cards.
1	5	Improve graphics used on the board.	The board in round two was designed using Canva, rather than PowerPoint, allowing for more flexibility in terms of graphics used.
1	6	Board layout improvements.	The layout of the playing board was altered to allow for a race to the centre to signal a clear win; other aspects of gameplay were added on to the board (such as the devices) to allow for more structured gameplay
1	7	Reduce words, improve clarity of cards.	Text on cards substantially reduced: scenarios made shorter, more graphics introduced to allow for easier interpretation.
1	8	Simplify cards to remove actions that were ignored in the gameplay.	Cyber Security cards no longer have costs or time spent associated with their purchase.
1	9	Standardise prizes won.	Answering a Quiz correctly results in one prize.
1	10	Make Quiz questions have closed-ended answers.	Quiz questions were reworded so that no questions require listing out of answers to win.
1	11	Alter the appearance and role of the data cards.	Data cards substantially reworked. The confusing flow between team and manufacturer and "data exposed without your consent" square removed, so that now teams just lose data. Cards changed in appearance to become round, interchangeable tokens.
2	12	Make the link between Device and Cyber Security cards clearer.	Device cards made bigger (to A7 size) and include three suggestions as to possible Cyber Security cards that might protect against attack.
2	13	Tighten up aspects of Cyber Security Battle.	Rules around card reuse made clear in the instructions (use the card, then replace with a new one from the pile) and how payment for losing works (losing team plays winning team). Change ratings from numbers to stars.
2	14	Board layout improvements.	Make the playing space bigger, and increase money and data tokens accordingly. Relabel "data breach" squares to reflect more specific cyber security failures.

In round two, special squares were introduced. Designated by being a golden colour with a red border, there was one of these special squares for each type of activity in the game (Quiz, Inside Threat, Outside Threat, and a new activity, Cyber Security Battle, which will be discussed below). See Figure 24 for a layout of the board. Winning, or protecting themselves in each of these special squares would allow the team to collect a piece to put into the newly designed 3D printed counters, shaped like a shield (an idea suggested by R1L7AM). Although there were four pieces to collect before heading to the centre to win overall, the rules did not specify that pieces had to be won on each of the four special squares (given the ongoing element of chance involved in being able to protect yourself from an Inside or Outside Threat). See Figure 20 for the new counters and wedges. It should still be noted, however, that it was also possible to lose the game, as before, by running out of money or data tokens, in much the same way as round one (through being unable to protect yourself). Requirements to give away money just as a result of landing on a square were removed in round two.

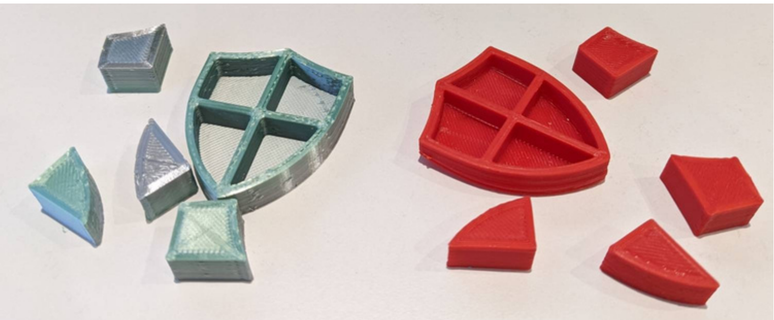
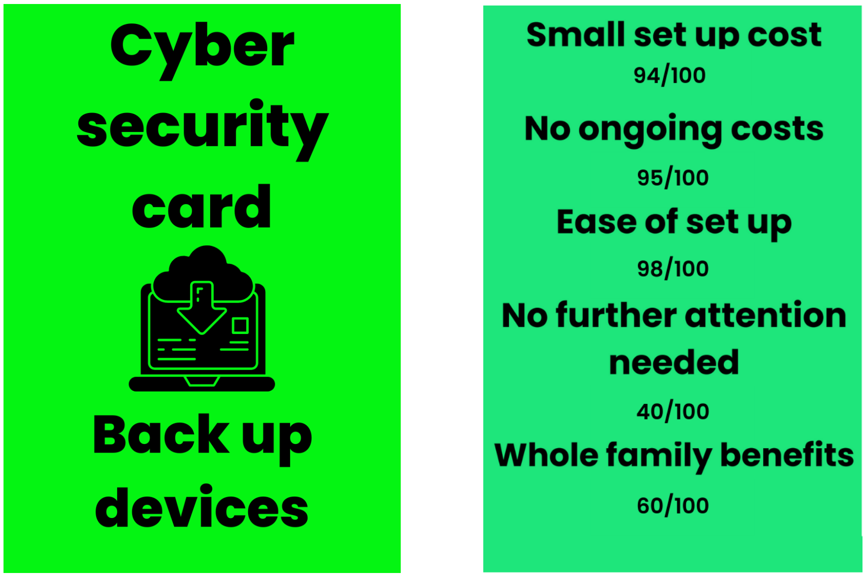


Figure 20: Updated counters and wedges

As mentioned above, several of the same activity features from before remained. Outside Threat and Quiz remained unchanged in their role in the gameplay. One activity was introduced and another altered to satisfy **Improvement 3**. The Cyber Security Battle activity was introduced not only to increase the adversarial aspects of gameplay, but also to help incorporate more consideration of the different ways in which Cyber Security cards could be more or less valuable. When landing on a Cyber Security Battle square, the team had to pick one of their Cyber Security cards, which now had five categories, with scores out of 100 on the back: Small setup cost; No ongoing costs; Ease of set up; No further attention needed; Whole family benefits (from the cyber security measure). Picking one of those categories, they would then challenge the other team to pick up one of their Cyber Security cards and look at the chosen category. The card with the higher number would win; the other team would lose £10. For an example of a Cyber Security Battle card, see Figure 21. In order to allow for ratings (an example from round two, with ratings given out of 100, can be seen in Figure 21) that did not overlap (ending in a stalemate), the researcher devised the ratings based on their relative understanding of the merits of each measure. For example, tape over camera had a higher "ease" score than setting up a guest network due to the need (or lack of) skills to set up. Although, ultimately, these were subjective decisions on the part of the researcher, the ultimate aim was to get participant families to start recognising that not all cyber security measures are the same in terms of setup and value, and to prompt discussions about whether they agreed.

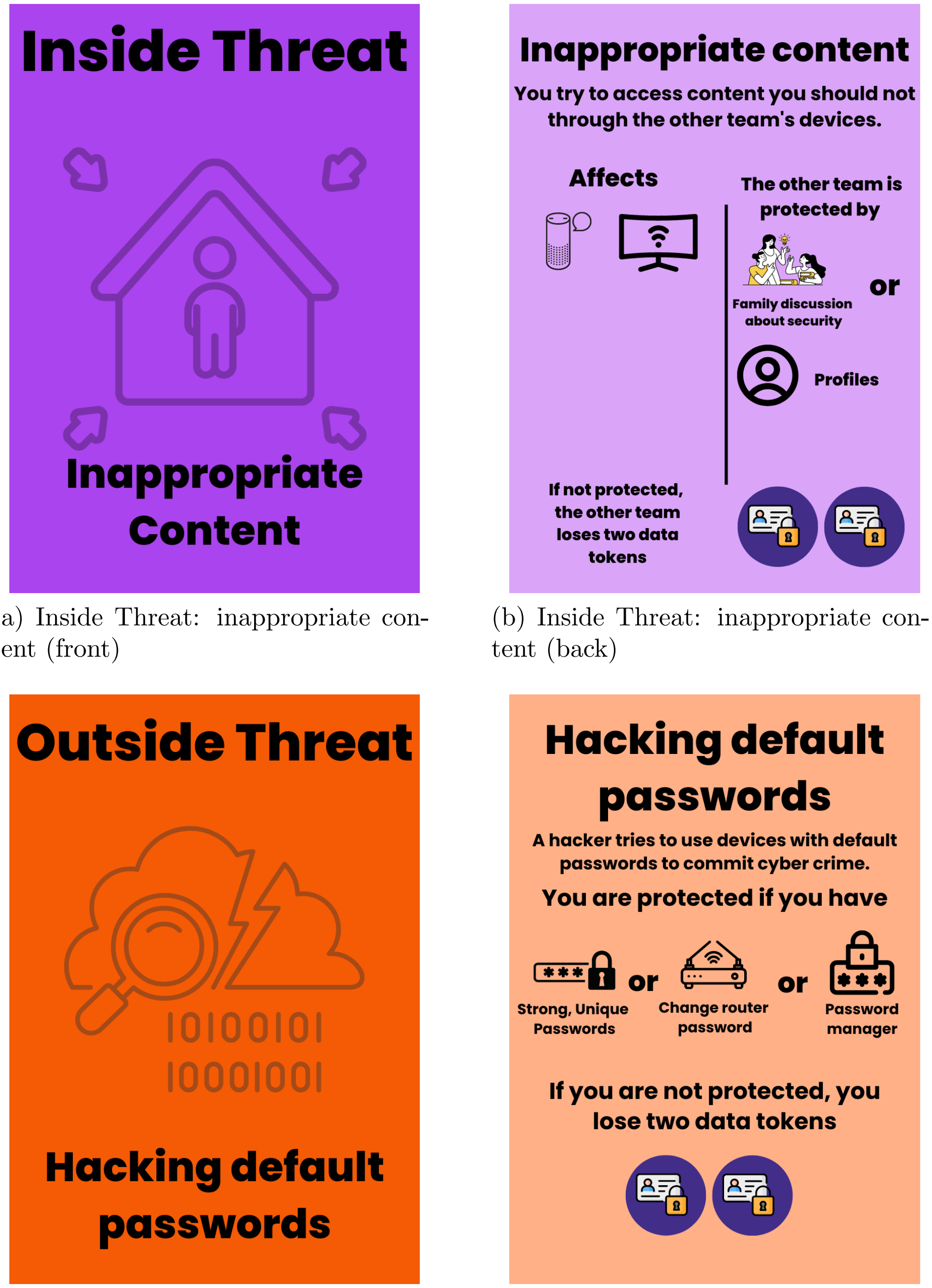


(a) Cyber Security card: front

(b) Cyber Security card: back

Figure 21: Cyber Security Card with first version of Cyber Security Battle back

The Inside Threat activity was altered, following the ideas brought up by Family R1K3, so that each team started with five Inside Threat cards each (see Figure 22 for updated cards). When a team lands on an Inside Threat square, they have to protect their devices from an Inside Threat attack from the other team, rather than pick up another card from the deck on the board (as previously).


Inside Threat
Inappropriate Content
Inappropriate content
You try to access content you should not through the other team's devices.
Affects
The other team is protected by
Family discussion about security
or
Profiles
If not protected, the other team loses two data tokens
Outside Threat
10100101
10001001
Hacking default passwords
Hacking default passwords
A hacker tries to use devices with default passwords to commit cyber crime.
You are protected if you have
Strong, Unique Passwords
or
Change router password
or
Password manager
If you are not protected, you lose two data tokens

(a) Inside Threat: inappropriate content (front)

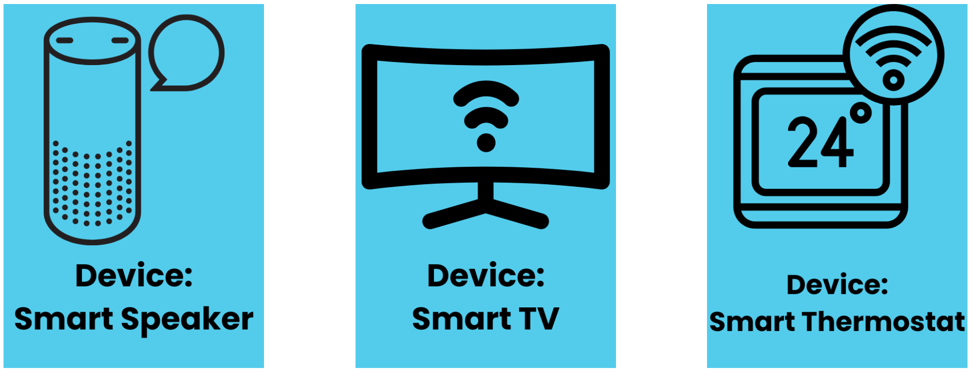
(b) Inside Threat: inappropriate content (back)

(c) Outside Threat: hacking default passwords (front)

(d) Outside Threat: hacking default passwords (front)

Figure 22: Round two: new Inside and Outside Threat cards

At this point, it is helpful to discuss **Improvement 4**, introducing more devices into the game. The counters used for moving around the board have, as mentioned above, been swapped with shield-shaped ones. More devices, as suggested by a number of families, have been explicitly added as part of the gameplay. Twelve devices (all strictly things in the home with Internet connectivity that are not typically considered to be technology products; no laptops or smartphones included) were introduced as small blue cards (see Figure 23). They were designed to be included, in particular, in relation to the process of the Inside Threat activity. The devices here serve two purposes at the same time, in terms of underlying messages: firstly, not all Inside Threats attack all devices, so sometimes an attack might be made by a team just to find that it fails because the other team simply does not have the device(s) that could be affected. Secondly, the introduction of specific devices started to underline that not all cyber security measures will work for all devices. In round one, the link had been made (with both Inside and Outside Threats) that not all cyber security measures will stave off all threats, but this took the link somewhat further, to include the fact that the usefulness of the cyber security measure would be dependent upon the device too. Squares to change a device were added to ensure a relatively frequent alternation of devices that would require different cyber security measures to keep safe. It was hoped that teams might start to strategise about which devices they wanted to pick up, based upon their knowledge of the cyber security measures that they owned.



(a) Smart speaker (b) Smart TV (c) Smart thermostat

Figure 23: Round two: new Device cards

Board, cards and pieces

The layout and look and feel of the board changed significantly between rounds one and two. These stemmed both from **Improvements 5 and 6**, but also from the desire to make the board feel more like a board game board. In terms of the design of the board, the second version of the board was designed in Canva,[2] a design tool allowing for a much more flexible approach to size and design, as well as providing access, in its paid-for version, to a significant graphics library. This allowed for a wider range of tools to make the board feel more like a genuine board game. The shape of the board was altered to that of a standard board game (50.2cm by 50.2cm); an image was added as a base underneath the gameplaying space, and the layout of the board, to allow for the altered gameplay, was created with additional areas for positioning of the device and data tokens in particular. As suggested in round one, the place on the board where players were to put their lost data was changed from a rectangle to a graphic that resembled a rip in the board, to signify something sinister and scary about losing the data. Once created, the board was then assembled using a standard blank board game board, and a custom printed vinyl sticker, with the board printed to size on it. The sticker was then carefully stuck to the board game board, and scored and cut as necessary to allow the board to fold up. This immediately gave the impression of a more professional-looking game than the foam-board board of round one.

Improvements 7, 8, 9 and 10 were all made to the appropriate cards. In particular, words were significantly reduced. This resulted in the removal of text doing the job of explaining about cyber security measures, or perhaps giving more background as to scenarios laid out in the Outside and Inside Threat cards. Information, where possible, was relayed through images. This was possible because of the ongoing use of a specific image for each cyber security measure, and similarly an image for each newly introduced device. When payment or data loss was mentioned as the outcome of failure to protect yourself in an Outside or Inside Threat, images of money (along with an amount) and/or images of data tokens were put on the cards (see Figure 22). This helped to standardise some of the actions in the gameplay, requiring less time to stop and understand the unique outcome of the specific card at hand, as was the case in round one. Similarly, Quiz

[2] `https:/www.canva.com`

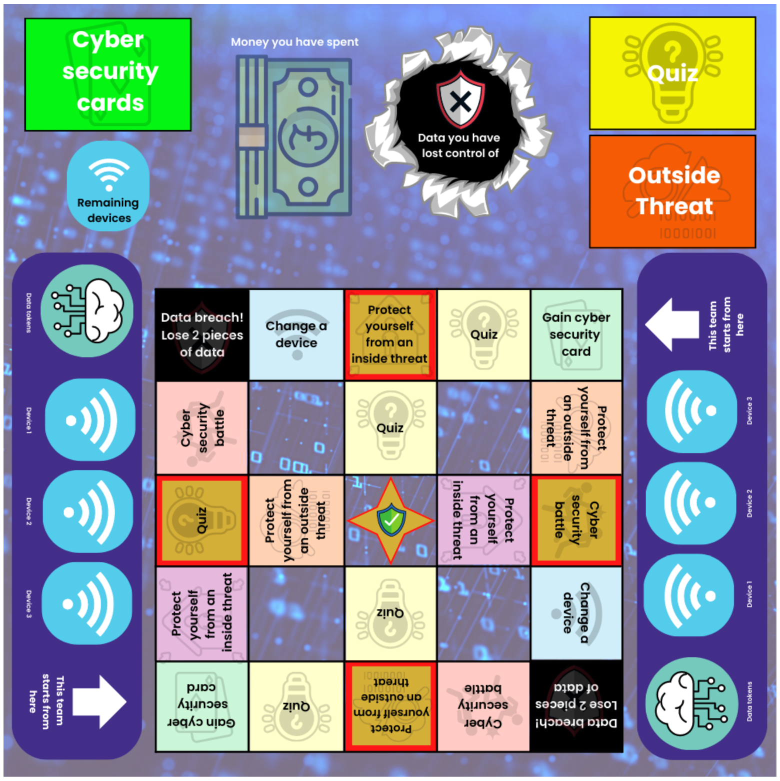

Cyber security cards
Money you have spent
Data you have lost control of
Quiz
Outside Threat
Remaining devices
Data tokens
Device 1
Device 2
Device 3
This team starts from here
Data breach! Lose 2 pieces of data
Change a device
Protect yourself from an inside threat
Quiz
Gain cyber security card
Cyber security battle
Quiz
Protect yourself from an outside threat
Quiz
Protect yourself from an outside threat
Protect yourself from an inside threat
Cyber security battle
Protect yourself from an inside threat
Quiz
Change a device
Gain cyber security card
Quiz
Protect yourself from an outside threat
Cyber security battle
Data breach! Lose 2 pieces of data
This team starts from here
Device 3
Device 2
Device 1
Data tokens

Figure 24: Round two board layout

cards were given a single prize for a correct outcome (a correct answer allowed for the winning team to pick up a new Cyber Security card); Cyber Security cards no longer had the aspects of subscription, payment or time spent setting up. As described above, although the element of nuance about the specificity of each device had been removed, this concept was more engagingly picked up through the Cyber Security Battle. Cyber Security cards now had to be picked up from the top of the pile when the appropriate square was landed upon. Quiz cards, too, had the structure of some questions altered — although the premise of all the questions remained the same — so that every question was framed as a multiple choice, leaving no aspect of interpretation for both teams, both in answering them and accepting responses.

The role of data in the game was altered, in line with **Improvement 11**. Two aspects were altered: the flow described above, where teams had to give data to the manufacturer, and would have data “exposed without your agreement” both directly and then through the manufacturer was removed. In round two, data

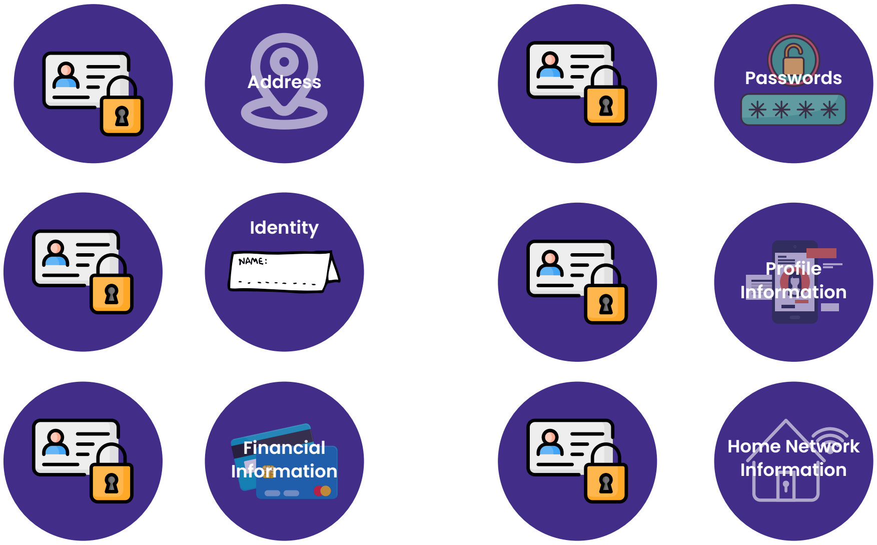


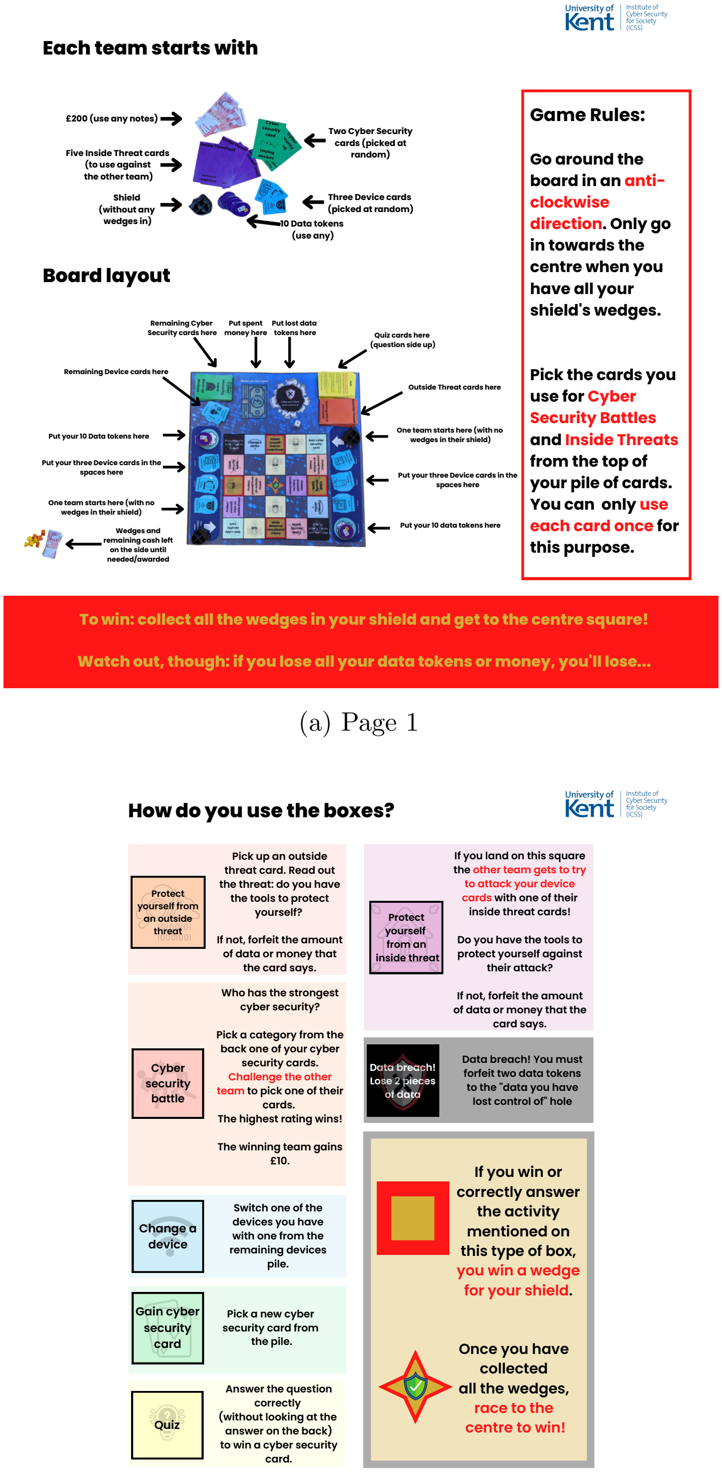
Figure 25: Examples of data tokens (front and back)

was lost directly as a result of failing to protect yourself in Outside and Inside Threats, or landing on the data breach squares, and placed into the space on the board for "data exposed without your agreement". Secondly, the representation of data was changed. It was no longer in A7 card form, rather the new data tokens were 2.5cm round tokens, with a standard graphic on one side representing personal data, and the second side with different, specific types of personal data, represented in both words and graphics (for examples, address, identity, search history). Although there were the specific types of personal data on the tokens, there was no requirement in the rules to start with or lose specific types.

Finally, one other small change was made to the game between round one and two. The instruction sheet was made more compact — a double-sided 20cm × 20cm page which was laminated (see Figure 26) — whilst working to ensure it was clearer than the previous version.

7.1.4 Round two feedback

Round two was played between August and September 2022, again with ten families. Seven of the families had taken part in the first round: this overlap was important to understand whether they were happy with the changes made between the rounds and if they considered those changes to be improvements. The



University of Kent | Institute of Cyber Security for Society (iCSS)

Each team starts with

£200 (use any notes)

Five Inside Threat cards (to use against the other team)

Shield (without any wedges in)

Two Cyber Security cards (picked at random)

Three Device cards (picked at random)

10 Data tokens (use any)

Board layout

Remaining Cyber Security cards here

Put spent money here

Put lost data tokens here

Quiz cards here (question side up)

Remaining Device cards here

Outside Threat cards here

Put your 10 Data tokens here

One team starts here (with no wedges in their shield)

Put your three Device cards in the spaces here

Put your three Device cards in the spaces here

One team starts here (with no wedges in their shield)

Put your 10 data tokens here

Wedges and remaining cash left on the side until needed/awarded

Game Rules:

Go around the board in an anti-clockwise direction. Only go in towards the centre when you have all your shield's wedges.

Pick the cards you use for Cyber Security Battles and Inside Threats from the top of your pile of cards. You can only use each card once for this purpose.

To win: collect all the wedges in your shield and get to the centre square!

Watch out, though: if you lose all your data tokens or money, you'll lose...

(a) Page 1

University of Kent | Institute of Cyber Security for Society (iCSS)

How do you use the boxes?

Protect yourself from an outside threat — Pick up an outside threat card. Read out the threat: do you have the tools to protect yourself? If not, forfeit the amount of data or money that the card says.

Protect yourself from an inside threat — If you land on this square the other team gets to try to attack your device cards with one of their inside threat cards! Do you have the tools to protect yourself against their attack? If not, forfeit the amount of data or money that the card says.

Cyber security battle — Who has the strongest cyber security? Pick a category from the back one of your cyber security cards. Challenge the other team to pick one of their cards. The highest rating wins! The winning team gains £10.

Data breach! Lose 2 pieces of data — Data breach! You must forfeit two data tokens to the "data you have lost control of" hole

Change a device — Switch one of the devices you have with one from the remaining devices pile.

Gain cyber security card — Pick a new cyber security card from the pile.

Quiz — Answer the question correctly (without looking at the answer on the back) to win a cyber security card.

If you win or correctly answer the activity mentioned on this type of box, you win a wedge for your shield.

Once you have collected all the wedges, race to the centre to win!

(b) Page 2

Figure 26: Gameplay instructions for the second round

three new families were also extremely important to serve as confirmation about the enjoyability and ability to learn from the game without having the first version to compare it to. The three new families all participated online. This was helpful as it allowed for a wider geographical range of participants; it also helped by creating a bit of distance between the researcher and the family as they played. The family knew, that as they played, the researcher would be watching (albeit with camera and microphone off) and be able to help if needed, but this offered more of an opportunity to explore the extent to which families could play the game, in their own home setting, largely by themselves.

As with round one, the feedback will be considered in terms of likes, dislikes and confusions, followed by specific suggestions for improvements.

Likes, dislikes and confusions

Likes:

Participants were broadly in agreement that this version of the game enabled **significant opportunities for discussion** to happen within the family as they were playing. The additional areas of adversarial play, the Cyber Security Battles and Inside Threat, as well as the continued favourite the Quiz, naturally provoked significantly more interaction between teams. *"I like the mixture of, almost like mini-games in between. I like that idea of a battle."* (R2K3AF); *"I quite like the way you're attacking their devices"* (R2O2AF).

> R2L6C2, aged 13: *[The Quiz questions] were good. Some of the terms were a bit confusing...*
> R2L6AM: *But it's good that it comes up and then if you don't know what it is we can discuss it.*

Some families also found that having to make decisions about the devices they wanted to have made for relatively strategic conversation — what device might you want given the Cyber Security cards that you held at the time? *"I thought this [device swap] was a good thing. Because you've got to make a decision about swapping, and what is the benefit? How is that making my team stronger?"* (R2L7AF).

The families playing the game for the second time uniformly agreed that the second version was **more engaging, straightforward to play, and better to**

look at, compared to the first round. *"The game was better visually, and better to play with"* Survey feedback from R2L10. *"I really liked the gameplay. I really thought it was very helpful, and it was quick and easy to set up and understand."*. *"This was definitely easier than the first round, as it wasn't as wordy."* Survey feedback from R2L7.

Unsurprisingly, the **ability to win, in addition to the additional competitive aspects**, was also popular. *"It's nice to have an end point [now]...it makes it feel more enjoyable"* (R2K1AM). That said, the ability to win was not without issues, as in the majority of cases, the game was not close to finishing when the 30 minutes finished. A number of participants commented along the lines of *"Maybe you want to make it a bit easier to win...[but] I don't really know [how]"* (R2O1C1, aged 13). *"I wasn't quite sure how long [you expected it to take] people to get into the centre."* (R2O1AF).

Dislikes and confusion:

As mentioned above, the benefit of having a game designed to be won came as a double-edged sword. Participants commented that, because of the element of chance in having the right devices and Cyber Security cards, it felt really quite **difficult to win pieces for the counters** (a precursor to being able to win) on the Inside and Outside Threat special squares (as noted above, though, there was no rule that said that pieces had to be gained from each special square). *"I thought it was going to be very hard to win a piece because sometimes you don't have the right device...so even if you were doing the right things, you couldn't possibly win. Not that I'm bitter."* (R2K1AF); *"I thought it was difficult to get the [pieces] though."* (R2K3AF).

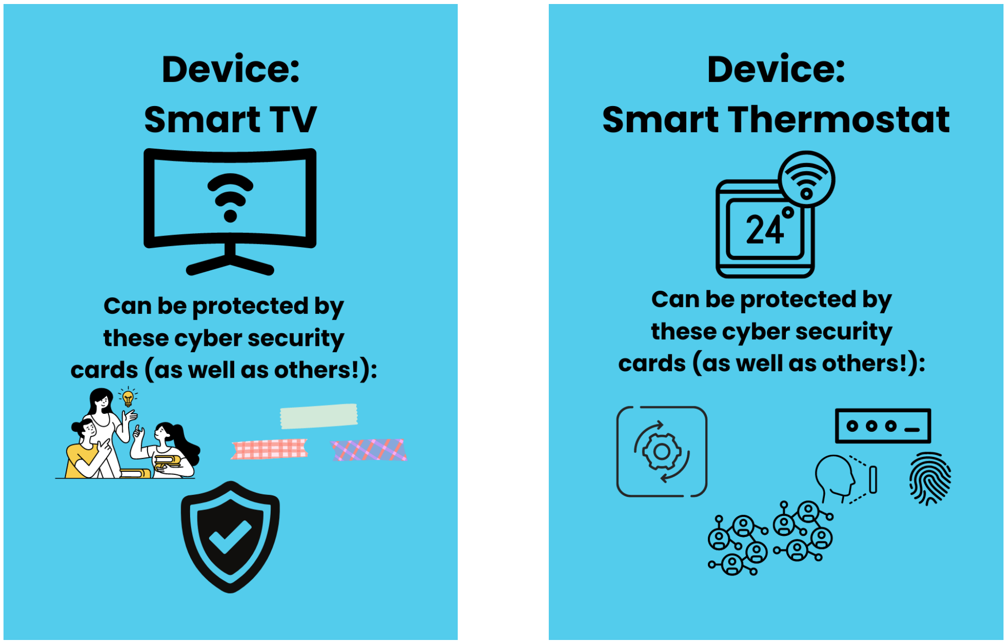
Linked to this in some participants' minds was the fact that the size of the **gameplaying space as a proportion of the entire board was too small** (*"It was a very small board!"* (R2L6C1, aged 12)) — the thinking here being, in some part at least, that more squares might help make it easier to win *"I think it should be a bit bigger, so it's easier to win...just a bigger board."* (R2L10C1, aged 14).

Certain aspects of the newly introduced **adversarial play needed further clarification**. In particular, whilst participants enjoyed the Cyber Security Battles, there was a lack of clarity in the instructions about what to do with the card used for the battle, particularly as some participants realised that, because of the relative laxity of the rules, they could retain a high-scoring card and keep using it to win almost any battle. One participant, R2O1C2, aged 11, suggested a way to deal with this: *"Could you [alter the rules] so once you've used one you like, swap it for another one?"* This was an excellent idea for two reasons: not only did it solve the immediate problem, but, going into the third iteration of the game, it required teams to have a continually evolving calculus as to which devices to have based on their Cyber Security cards, and vice versa.

Also in family R2O1, C1, aged 14, pointed out **how confusing it was to have scores in the Cyber Security Battle that were numerical**, particularly when two of the categories related to cost. The card's rating worked on the basis that higher the rating out of 100, the better the measure was for its user. Of course, with cost, the higher the rating, typically, the lower the cost, which can feel contradictory. R2O1C1 suggested *"Stars, maybe? I think maybe [rating out of] 10 stars would be good."* It was also agreed that the two cost categories should be rolled into one, given the similarities of the figures in a number of cases.

The removal of significant amounts of text was one of the most agreed-upon requests of round one and commented on as an improvement for many, as noted above. This, however, lead to confusion in round two. In particular, **some participants missed the brief explanation given on Cyber Security cards**, which had been removed to avoid having overwhelming amounts of text. In general, however, it was noticeable how much easier the reduced amount of text, and increase in the number of images in the text's place, helped facilitate gameplay. Children no longer stumbled over long passages of words. Importantly, too, comments around the need for more information allowed the researcher to point out the inclusion of the explanation booklet (See Appendix P), a resource typically overlooked by participants.

Finally, despite the inclusion of data tokens being better received than the initial data cards, many participants still commented that **the concept of the data, and the importance surrounding the loss of data, felt quite remote**. In part, this may have been related to the squares the participant landed on — not all threat cards, for example, would result in the loss of data. Fundamentally, the issue from round one remained — participants could conceptualise the loss of money much more easily than the loss of data. To that end, R2O2AM suggested that two of the squares — the black squares that automatically lost



(a) Updated smart TV Device card

(b) Updated smart thermostat card

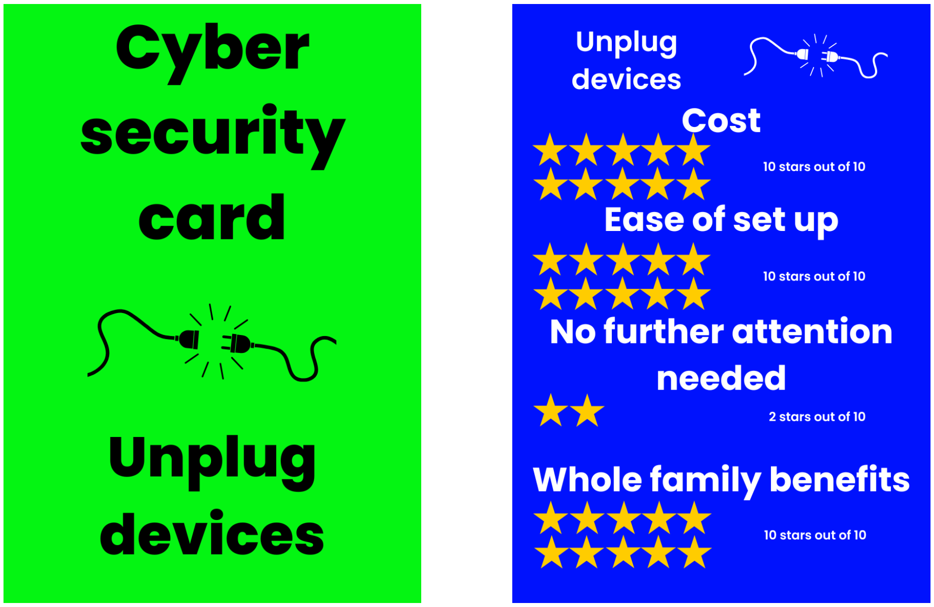
Figure 27: Updated Device cards

participants' data tokens by virtue of landing on the square — could provide a learning opportunity to reflect how poorly people keep their data secure. *"So rather than data breach, lose two pieces of data: maybe it's like 'you forgot to back up'."*

Improvements suggested

The improvements suggested from round two were very minor in relation to those coming out of round one. These are listed out below, along with pictures of the changes made. For an overview of all the changes made, see Table 21.

Improvement 12: Make the link between Device and Cyber Security cards clearer. Participants generally appreciated the inclusion of the devices to the game, but there was a recognition that the links between the Cyber Security cards and the devices that they were protecting were not immediately obvious. This was in part because there was no mention on the Device cards as to which Cyber Security cards might protect them; but also, as players were required to pick up the next Cyber Security card when the option arose, as R2K1AF put it,



(a) Updated Cyber Security card: front

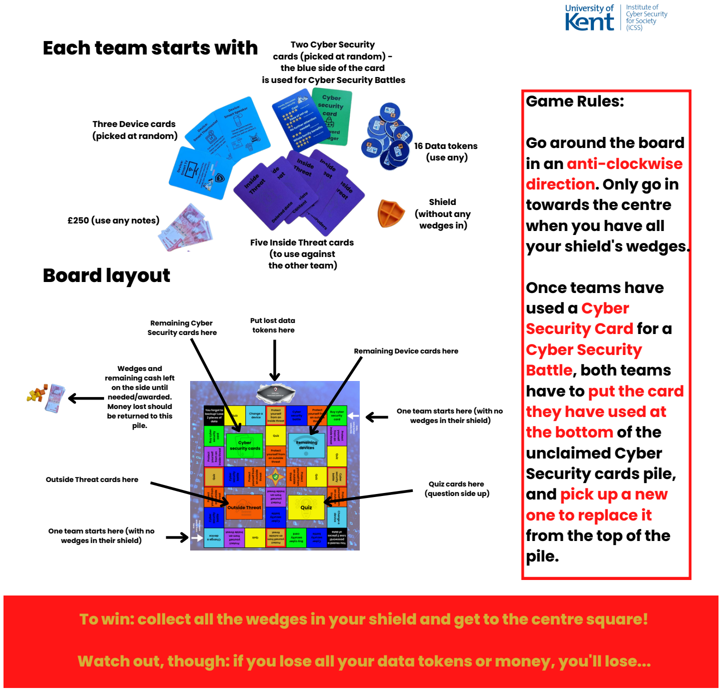
(b) Update Cyber Security card: back

Figure 28: Updated Cyber Security Card with Cyber Security Battle back

"sometimes [it is] a bit random, you've got [Cyber Security cards] that don't relate to the devices you have". For round three, three potential cyber security measures relevant to the device were added to the Device cards (see Figure 27).

Improvement 13: Tighten up aspects of Cyber Security Battle. Rules around the reuse of cards were made clearer in the game rules, with ratings being changed to stars out of ten (see Figure 28). The determination about how to rate the categories remained the same as described in Section 7.1.3. Also, tightening up the rules to ensure that the losing team pays the winning team in any one battle. These were reflected in the new version of the game rules (See Figure 29).

Improvement 14: Board layout improvements. It was suggested that the gameplaying space on the board should be bigger — and so the additional features added on to the board — as suggested in Improvement 6 — were rolled back. The number of squares was increased as a result, and in line with this, the amounts of Data tokens and money provided to each team at the start of the game were increased. Finally, the "data breach" squares were relabelled to reflect the idea of losing data because of commonly poorly adhered to cyber security practices (not backing up and reusing a password). These can be seen in the board (see



Each team starts with

Two Cyber Security cards (picked at random) - the blue side of the card is used for Cyber Security Battles

Three Device cards (picked at random)

16 Data tokens (use any)

£250 (use any notes)

Shield (without any wedges in)

Five Inside Threat cards (to use against the other team)

Board layout

Remaining Cyber Security cards here

Put lost data tokens here

Remaining Device cards here

Wedges and remaining cash left on the side until needed/awarded. Money lost should be returned to this pile.

One team starts here (with no wedges in their shield)

Outside Threat cards here

Quiz cards here (question side up)

One team starts here (with no wedges in their shield)

Game Rules:

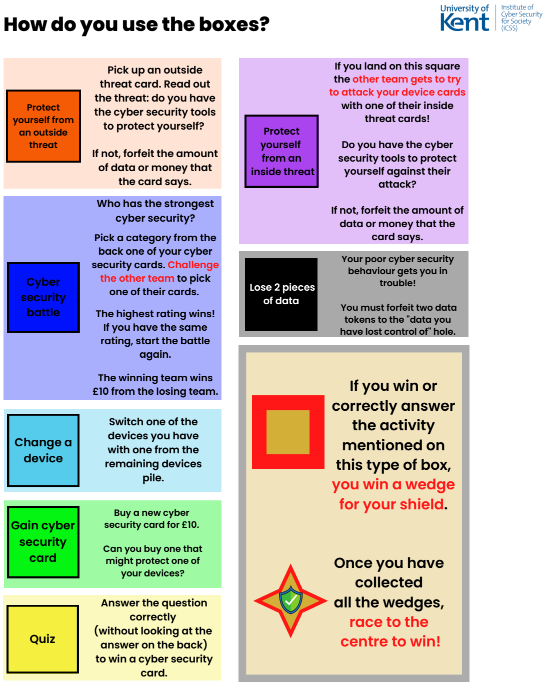
Go around the board in an anti-clockwise direction. Only go in towards the centre when you have all your shield's wedges.

Once teams have used a Cyber Security Card for a Cyber Security Battle, both teams have to put the card they have used at the bottom of the unclaimed Cyber Security cards pile, and pick up a new one to replace it from the top of the pile.

To win: collect all the wedges in your shield and get to the centre square!

Watch out, though: if you lose all your data tokens or money, you'll lose...

(a) Page 1



How do you use the boxes?

Protect yourself from an outside threat: Pick up an outside threat card. Read out the threat: do you have the cyber security tools to protect yourself?

If not, forfeit the amount of data or money that the card says.

Protect yourself from an inside threat: If you land on this square the other team gets to try to attack your device cards with one of their inside threat cards!

Do you have the cyber security tools to protect yourself against their attack?

If not, forfeit the amount of data or money that the card says.

Cyber security battle: Who has the strongest cyber security?

Pick a category from the back one of your cyber security cards. Challenge the other team to pick one of their cards.

The highest rating wins! If you have the same rating, start the battle again.

The winning team wins £10 from the losing team.

Lose 2 pieces of data: Your poor cyber security behaviour gets you in trouble!

You must forfeit two data tokens to the "data you have lost control of" hole.

Change a device: Switch one of the devices you have with one from the remaining devices pile.

If you win or correctly answer the activity mentioned on this type of box, you win a wedge for your shield.

Gain cyber security card: Buy a new cyber security card for £10.

Can you buy one that might protect one of your devices?

Once you have collected all the wedges, race to the centre to win!

Quiz: Answer the question correctly (without looking at the answer on the back) to win a cyber security card.

(b) Page 2

Figure 29: Gameplay instructions for the second round

Figure 30) and reflected in the new version of the game rules (see Figure 29).

Three suggestions, or areas of concern, mentioned above were not changed in the third round. Although it remained a concern, the fact that it was proving difficult to win (although two of the ten families did have a winning team) felt, in some respects, less of a concern from a research point of view, as it allowed for a sufficiently long period of time of consistent play. It also should be considered against estimated times for other popular commercial games, which can often take several hours to complete. There was no addition of extra text on the cards, again with the understanding that any confusion should be a good driver to review the explanation booklet. Finally, although participants still reported being unsure of the value of the Data tokens, these remained the same (albeit increased in number) in the final round, as the difficulty of conceptualising data, relative to money, seemed to be an important finding that could not be fixed simply within this game, without compromising other lessons to be taken away from the game (notably, removing the need to pay as well as losing data).

The final set of cards used in round three can be found in Appendix Q.

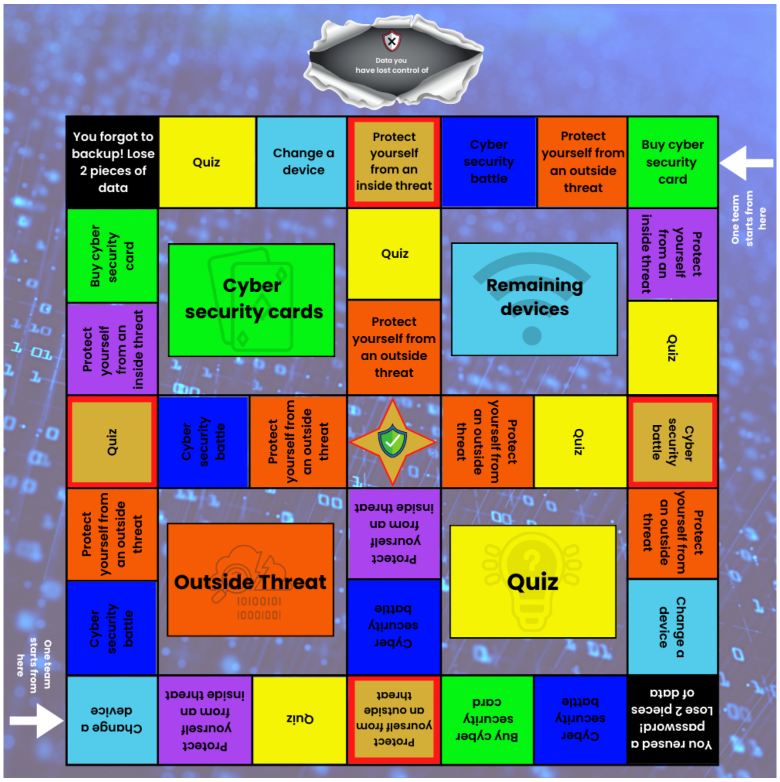

Data you have lost control of
You forgot to backup! Lose 2 pieces of data
Quiz
Change a device
Protect yourself from an inside threat
Cyber security battle
Protect yourself from an outside threat
Buy cyber security card
One team starts from here
Buy cyber security card
Cyber security cards
Quiz
Protect yourself from an outside threat
Remaining devices
Protect yourself from an inside threat
Protect yourself from an inside threat
Quiz
Quiz
Cyber security battle
Protect yourself from an outside threat
Protect yourself from an outside threat
Quiz
Cyber security battle
Protect yourself from an outside threat
Outside Threat
Protect yourself from an inside threat
Quiz
Protect yourself from an outside threat
Cyber security battle
Cyber security battle
Change a device
One team starts from here
Change a device
Protect yourself from an inside threat
Quiz
Protect yourself from an outside threat
Buy cyber security card
Cyber security battle
You reused a password! Lose 2 pieces of data

Figure 30: Round three board layout

Round three

Round three, being the final round in the research, was focused less on eliciting feedback for improved gameplay, and more on the cyber security learning from the game. The third round was additionally valuable in being played by an entirely new group of families, who had not been involved in the previous rounds at all. All the sessions were undertaken online, too, which, as described previously, enabled the researcher to be more remote, and look at how well gameplay could be facilitated by the families themselves. This section will be structured in the opposite way to rounds one and two, in that there will be a very brief overview of dislikes and confusion before moving on to likes.

Dislikes and Confusion:
Very few issues were raised in the follow-up survey; in all cases, these were issues that had been raised in the prior rounds. There were **requests for continued clarification of game rules** (around the Cyber Security Battle and when to be able to move through the centre of the board); there were two comments referring to the fact that **it felt like the game may be hard to win**; there was also one comment referring to the continued **difficulty of understanding what the Data tokens were**: *"We didn't know what the tokens were for and wondered if they were needed as the monetary fine seemed to be enough"* (R3O8).

Likes: The explicitly positive feedback came from the survey, rather than in game sessions.

> *We really enjoyed the game! We play lots of board games and get very competitive. It was a great opportunity to talk about digital safety without actually forcing the children to have a conversation.* (R3O4)

> *It is excellent; I would recommend.* (R3O5)

> *We enjoyed playing the game together, and it did provoke further discussion about passwords and not making them all the same thing or sharing them.* (R3O8)

> *We all enjoyed playing the game, and I think it made the adults more aware of some things than the kids, as they've had lots of info at school.*

> *The layout was very engaging, and we actually did say later on that it would be fun to play again!* (R3O9)
>
> *We thought it was excellent!* (R3O12)
>
> *We really enjoyed the game.* (R3O13)

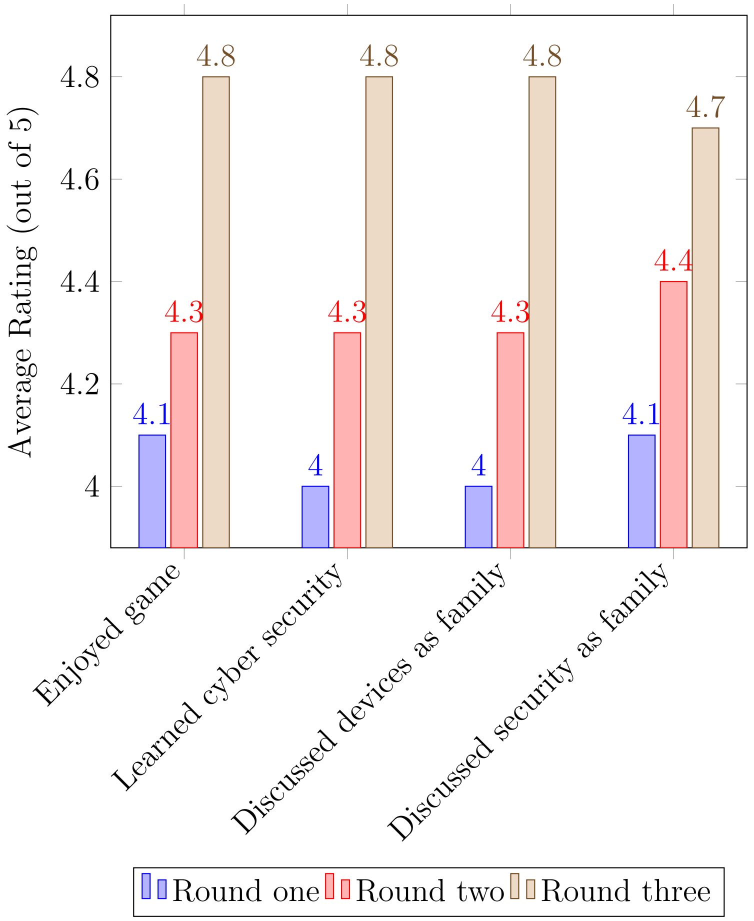
This is clearly a good indication that the UCD process worked to produce an enjoyable game that could be learned from — particularly as participants in round three were new to the game itself. As an onlooker, it was clear to see that the game created engagement — in three cases, families begged for more time to continue playing after the half an hour was up; one family reported that they had waited until the end of the research session to play until completion afterwards.

Participants were asked, as part of the feedback survey, to rate whether they thought that the game had helped knowledge and discussion around cyber security, as well as rating their enjoyment of the game. It is clear to see the higher ratings given for the final version, as shown in Figure 31. The ratings between rounds two and three show, in quantitative terms, negligible changes, compared with rounds one and two. This is actually a positive finding, when it is considered that seven of the families participating in round one also participated in round two: the ratings show a clear improvement between rounds one and two. Round three, undertaken with entirely new participant families, underlined the fact that the incremental changes between rounds two and three made for a better game still — even with no experience of the games used in the previous rounds. In this respect, RQ4a — "Can UCD with families create an increasingly engaging board game that increases awareness of cyber security?" — seems to have been positively answered.

7.1.5 Cyber security findings

As well as testing the ability to participate in the design of an engaging version of the game, RQ4b and RQ4c asked if families could improve their cyber security knowledge in the short term and their cyber security standing in the home as a result of playing the game over a longer-term. This section will report back on the findings of this by analysing the data provided by families from data collected in the game, and also from the feedback survey, to see if all versions of the game

Figure 31: Average participant ratings from post-game survey



produced cyber security learning opportunities (and if any were noticeably better at doing so) based upon this feedback. Then, to understand if the game was more successful at engendering changes to cyber security standings than if it had not been played, answers from the feedback survey will then be compared to the control group answers, to see if the families playing the game were more likely to have changed aspects of their home cyber security setup than the control group in the week following the gameplaying session.

How successful were the games at widening participants' understanding of cyber security?

This section will use answers given by participants at three points during the gameplaying cycle: the pre-game questionnaire, the post-game questionnaire, and the feedback survey, filled in a week after gameplay. The questionnaires were used to understand whether playing the game gave any immediate boost in knowledge, and in particular, if certain concepts of the game were more likely to "stick" with participants; looking to answer RQ4b. The feedback survey, performed, as it was, a week later, was intended to show whether or not that the game had served as a means of facilitating a change in cyber security practices at home; looking to answer RQ4c. It should be noted again that in one case, a family did not fill in the feedback survey (R1L4) — this means that, when considering information from the feedback surveys of round one, there will only be nine surveys, not ten. In another case, in round three, a participant family had a parent who worked in the cyber security industry: this family's results were different from other participants, in that they had implemented, or had knowledge of, almost all of the learning aspects of the game ahead of time, because of the parent's professional knowledge. In this case, a lack of action was not because of a lack of interest, but rather, a recognition that they needed to make no changes to their current setup.

Did playing the game extend the family's knowledge?

The game introduced players to three main ideas: data types, threat types, and cyber security measures. The pre- and post-game questionnaires allowed for an opportunity to see if participants' understanding of these widened as a result of playing the game. Looking at the responses, it would be possible to see if a wider range of types were given in the post-game questionnaire; in particular, concepts lifted from the game. A wider range of data types and threats being recorded post-game would show — even if only in the period immediately after the gameplay — that the participants had learned additional elements of each category compared to before gameplay. The range of responses, rather than the number of responses, were used, as the post-game responses were filled in after participants had been concentrating for nearly an hour, leading to more briefly answered questions in all cases. Responses are considered at the round level (so, across all participants in the named round) unless otherwise stated.

Data types

Participants were asked "what is worth protecting on your smart TV/streaming device/smart home assistant?", and were told to interpret the question however they wanted (should they have asked the researcher for guidance). Participants' responses were coded against the data types provided on the data tokens in rounds

Table 22: Reported data types pre- and post-game by participants by round

	Round one		Round two		Round three	
	Pre-game	Post-game	Pre-game	Post-game	Pre-game	Post-game
Address	1	1			1	1
Contact Information				1		2
Demographic information						3
Employment history						3
Financial information	7	5	11	5	3	4
Identity	13	10	25	9	15	4
Message history		1			1	2
Network information			4	3		3
Passwords	7	6	11	5	8	4
Personal safety	1	1				
Photos	2		2		4	
Physical device	2					
Privacy	1	1	4	1	1	1
Profile Information		5				2
Purchase information	2		2		3	2
Search history	1		2	3	3	3
Voice data			2	1	2	
Count of data types reported	10	8	9	8	10	13

two and three, to allow for uniformity of answers, where possible.[3] Three answers provided by participants were not coded against these types: "privacy", "personal safety" and "photos", as they did not correspond directly. "Personal safety" and "photos" were recorded in the pre-game questionnaires only: "privacy" — an extremely broad concept — was recorded in all pre-game questionnaires, as well as post-game questionnaires in rounds two and three.

It is perhaps indicative of the different focus on data in the first round of the game, with the larger Data cards rather than tokens, that participants did not obviously learn from the game, being able to name nine data types in the pre-game questionnaire, and only eight after (see Table 22). Round two found more of an improvement, with eight data types named beforehand, and nine afterwards. Round three showed the biggest improvement, with eight data types named in the pre-game questionnaire, and thirteen in the post-game questionnaire. Online families (in rounds two and three) were able, on average, to produce more data types in the post-game questionnaire than offline families. Round one's average (all offline families) in the post-game questionnaire was 3 data types; round two offline was 2.7, with round two online providing, on average, 3. Round three (all online) participants provided an average of 3.4 data types afterwards. As mentioned above, "personal safety" and "photos" were not included post-game, but "demographic information", "employment information", "contact details" (such

[3] The data types provided in rounds two and three were detailed out by data type rather than grouped together at a higher level, as in round one.

as telephone numbers) and “profile details” were included for the first time in the post-game questionnaire, suggesting a widening of understanding in rounds two and three.

Threat types

Participants were asked “Who do we want to protect [what we want to protect] from?” This question corresponded to the Inside and Outside Threat cards in the game, and it was hoped that the inclusion of Inside Threats in particular might help participants think more broadly than the “hacker in a hoodie” that came up so prominently in Chapters 4 and 5.2. Round one had the same number pre- and post-game — six each time, with one new category introduced: that of “guests in the home”. This meant that the post-game questionnaire had marginally more threats that emanated from inside the home. Rounds two and three had a much clearer distinction pre- and post-game: round two went from seven groups pre-game to twelve post-, and round three went from five pre-game, to eight post-. New groups included in the post-game questionnaire were “acts of God”, “burglars” and “power surges”, all of which were aspects in the game (see Table 23). There were, as well, significantly higher numbers of participants referencing threats posed by “pets” and “guests in the home”, which were, again, threat aspects in the game. Online families fared worse at this task, on average, compared to offline, with round one (all offline) participants averaging 2.22 threats after the game; round two saw offline participants produce 3.13 threats on average, and online 1.66; in round three (all online), participants listed 2.20 threats. It is interesting to note that, although “online data collection” was referenced, at no point did any family reference “manufacturers” as an entity that they would want to protect from.

The Inside Threat cards often prompted amusement and further discussion: one family discussed how their teenage son had kicked a drink over a laptop whilst sleeping (which prompted him to be more careful in future)(R2O2); another had an in-depth discussion about the merits of having a board with their Wi-Fi password at the front door (to stop having to explain it further to people)(R3O7); a third realised it would be helpful to talk to their relatives, who took guests in as AirBnB hosts, about how to provide guest Internet access without compromising their security (R3O4).

Table 23: Reported threat types pre- and post-game by participants by round

	Round one		Round two		Round three	
	Pre-game	Post-game	Pre-game	Post-game	Pre-game	Post-game
Acts of God				1		
Burglars				2		1
Family at home	1	4	2	3	3	2
Foreign Governments				1	2	
Guests at home	1		1	1		2
Hackers/scammers/criminals	10	8	17	10	14	9
Neighbours		1		2		3
Online data collection	2	3	7	2	5	2
Other people	4	3	7	4	1	1
Pets			1	2		2
Power Surge				1		
UK Government	3	1	1	1		
Count of potential threats reported	6	6	7	12	5	8

Hackers and scammers remained relatively popular potential attackers throughout, albeit with drops in numbers in the post-game questionnaire in rounds two and three (from 17 to 10, and 14 to 9 respectively), showing a widening of understanding of the types of threat beyond this. Notably, these were discussed far less frequently in the post-game activities. In fact, some children discussed how their friends had actually acted as they would consider hackers to, by stealing usernames (R1L4), spending other people's online currency in games (R2L6), and overriding school systems (R3O13).

Cyber security measures

Cyber security measures were addressed slightly differently, as the questions asked before and after gameplay were different. Participants were asked, before gameplay, "what do we currently do to avoid it [things we want to protect being taken by those we need to protect it from] happening?" and "Do we all do the same things?" After gameplay, families were asked "What do we all agree to do to keep the devices safer?"

In the most straightforward way, the families seemed to be aware, in general, that different family members approached cyber security differently; 19 of all families answered that they did not do the same thing. 13 said that they did; the remaining eight families disagreed within their answers (with one team saying yes, the other no), suggesting that there likely was some difference!

On average, across all families, 3.5 cyber security measures were listed as being used in the pre-game questionnaire (see Table 24 for overall figures of measures reported). The minimum number listed by a family was one, the largest nine. The most popular cyber security measures listed as being already used were "strong

Table 24: Pre-game reporting of cyber security measure use

Cyber security measure	Families reporting pre-game using the measure	Percentage of all families
Antivirus	7	23.33%
Back up	1	3.33%
Decline cookies	1	3.33%
Delete search history	1	3.33%
Discussion	2	6.67%
Don't interact with strangers	1	3.33%
Don't share login details	7	23.33%
Don't talk to strangers	1	3.33%
Don't use devices	1	3.33%
Don't use questionable websites	3	10.00%
Encryption	3	10.00%
Firewalls	3	10.00%
Limit online info	4	13.33%
MFA	4	13.33%
Not much	3	10.00%
Parental controls	4	13.33%
Parents control setup	1	3.33%
Passcodes	5	16.67%
Password manager	1	3.33%
Physical safety	2	6.67%
Read terms and conditions	1	3.33%
Strong passwords	19	63.33%
Unplug devices	1	3.33%
Use security	4	13.33%
VPN	2	6.67%

passwords" (listed by 19 families), not sharing login credentials (7 families), using antivirus software (7 families) and passcode usage on smartphones (5 families). When compared with the steps families decided that they would take (see Table 25), there is some overlap, particularly on passwords, which suggests that, in at least some cases, families may have written down that they used strong passwords in the pre-game questionnaire and perhaps realised that this was not a correct statement as the gameplay progressed. Of course, it is important to note that a larger number of measures may not, necessarily, imply a stronger security stance — as implied with the finding for passwords above, not all cyber security measures may be relevant or appropriate in a situation, or for a particular technology (or used consistently throughout all technologies).

One caveat that must be taken into account when considering the post-game intentions (and actions): where, as in the case of the family with the expert parent, the home setup was considered sufficiently secure, inaction is not necessarily to be considered a negative outcome. However, outside of the expert family, when comparing what families said that they would do in the post-game questionnaire,

Table 25: Post-game intention to implement cyber security measures

Cyber security measure	Families reporting intending to implement	Percentage of all families
Antivirus	5	16.67%
Automatic software updates	4	13.33%
Backing up	2	6.67%
Be more aware	4	13.33%
Care with Internet/devices	4	13.33%
Close down old accounts	2	6.67%
Family Discussion	3	10.00%
Firewalls/network traffic control	2	6.67%
Limit sharing of personal data	4	13.33%
MFA	3	10.00%
Parental Controls	2	6.67%
Passcode hygiene	6	20.00%
Password hygiene	13	43.33%
Password Manager	3	10.00%
Physical device safety	6	20.00%
Router password	2	6.67%
Tape over camera	2	6.67%
Unplug devices	4	13.33%

Table 26: Actual cyber security measures implemented by families in the week following gameplay

Cyber security measure	Measures implemented within week following gameplay	Percentage of all families
Antivirus	1	3.33%
Changes to be made imminently	3	10.00%
Closing old accounts	2	6.67%
Family Discussion	8	26.67%
Guest network	5	16.67%
Limit smart devices	1	3.33%
No changes made	9	30.00%
Parental Controls	1	3.33%
Password hygiene	6	20.00%
Password manager	1	3.33%
Physical device safety	1	3.33%
Router password	3	10.00%
Software Updates	1	3.33%
Tape over camera	1	3.33%
Unplug devices	2	6.67%

compared with what they said that they already do, the answers were more specifically focused towards cyber security measures that may have some impact on the home. Rather than giving the types of answers seen in the pre-game questionnaire (such as “VPNs” (2 families), “encryption” (3 families) or “use security” (5 families)), more specific measures were written down, in keeping with examples of good security practices provided on Cyber Security cards in the game: “use stronger passwords (or passcodes)” (13 families) “automatic software updates” (3 families), “unplug devices” (3 families), “close down accounts” (1 family), and “use tape over camera” (1 family).

In rounds two and three, seven of the ten families reported making, or imminently intending to make, modifications to the cyber security settings that they had in their homes (round one had 6 families reporting this). As mentioned, one family in round three did not make any changes because of the expert status of one of the adults playing, rather than through a lack of interest (they reported being happy that the game had reconfirmed that they were doing what felt appropriate for them). See Table 26 for overall figures of changes implemented. Interestingly, despite being given the post-game questionnaire as an *aide mémoire* in the week between gameplay and the follow-up survey, participants often reported making entirely different changes in reality, compared to what they had suggested they would do immediately after gameplay.

It is worth noting that the version of the game played seemed to make a small difference in the effect that gameplay had. Round one had, on average, 1.11 cyber security measures implemented. Of those in round two who played the game in person, the average number of changes made was 0.86 (which will be further discussed below). Online participants in round two made an average of 1.66 changes. Considering all ten families in round two together, the average number of changes made was 1.10. The participants in round three (all of whom were online) made an average of 1.60 changes. This seems to suggest two things: that round three seemed to be more effective at making participants make changes — but this is perhaps because online participation may have made making changes easier, or more likely, given the setting at home (as it was noted in both rounds two and three). It is important to note that the lowest average number of changes was in round two, where participants were repeating the gameplay process. Across the two rounds, these seven families (those that repeated gameplay in rounds one and two) reported making 12 changes (1.71 per family). Two families made no changes in either round. Two families reported starting a process in round one that was still ongoing in round two (one family was going through and closing old accounts, the other had set up a guest network and was still making the requisite changes when round two occurred). Four of the families reported making different changes after each gameplaying session. This suggests two benefits of repeated play of the game (albeit in different rounds) — the average number of changes made was higher amongst these four families (with an average of 2.5 changes per family across both games), almost certainly because they had the opportunity to make the decision to change their security practices twice — and seem to have taken advantage of it.

Of the families that participated, nine made no known changes after the event (as discussed, in at least one of these cases, it was because of the expert knowledge of one of the parents, who had already implemented the types of security measures discussed in the game; another family did not complete the survey).

As is laid out in Table 18, the game was relatively open in terms of the types of cyber security measures that participant families might decide to take away from the gameplay session. This allowed to gain an understanding of which types of security measures felt important — and which did not. It also allowed the opportunity to understand where participant families appeared to be on the TTM cycle. Having discussion bolstered with learning could be considered a vital first step to move from precontemplation to contemplation — that is, to recognise there might be a problem that needs to be solved. In fact, the most popular reported measure was the ongoing family discussion as a result of playing the game. Nine families reported discussing aspects that came up in the game in the immediate family group that had taken part, as well as amongst wider friends and family members too.

Following the TTM cycle, it would seem that a number of families moved beyond contemplation to action: implementing measures that seemed appropriate to them. Implementation of measures might show a movement through to action, but are the actions taken valuable in terms of creating a more secure home network? The results show that strong passwords were both widely considered to be already used, but also the most agreed to be implemented. Unsurprisingly, in line with the finding above that most families already thought that they used strong, unique passwords before gameplay, despite 13 families agreeing to do this, only six reported implementing changes relating to passwords. Although not possible in the remit of this piece of research, it would be interesting to follow up the extent to which this password changing was continued after the week-long period, which would reflect a slip from action into relapse in the TTM model, rather than maintenance. Similarly, changes to passcodes (on smartphones) were considered (in particular, to prevent younger children from opening up smartphones and apps), but were not reported as being implemented at all.

Other relatively popular reported actions appear to be one-time in setting up (four families reported setting up a guest network; three made changes to their router password (or its password availability for guests), and a fourth planned to do so imminently; one family reported tape over their smart device cameras). It should be noted that two further families looked into setting up a guest network and could not figure out how to make it happen. It is perhaps unsurprising that one-time actions were popular, and, in the case of the router password and putting tape over cameras, effective measures in terms of effecting tangible change (on the assumption that the passwords were strong and unique!). Guest networks, as discussed in Chapter 5 are complex, as they can often only be set up imperfectly: it is not clear whether those families that made changes did so knowing that complete isolation of home IoT devices from the other networked devices at home is not always completely possible.

Cyber security measures that required ongoing effort or potential spending money were reported less frequently. Three families reported unplugging their devices when not needed, although one reported that they were close to giving up because of the effort it took every time they used the device, perhaps suggesting that single-time actions are much more likely to be maintained than cause a relapse, in terms of the TTM cycle. Only one family reported actively looking to get a password manager for their children (and then because of the positive experience that one of the parents had had using a password manager for work).

These findings call for further consideration of the two most popular cyber security measures, strong passwords and family discussion, taking into account discussions in the gameplay itself.

Passwords: use and knowledge of strength

Participant families seemed to have an overly-generous belief that they understood what a strong password might practically look like, and how best to manage those passwords. They came up both prominently in the "things we currently do" *and* "things we will improve" sections for many families. Passwords have been recognised as a problem in usable security for almost as long as they have existed (with the earliest papers appearing in the 1970s (Morris and Thompson 1979), and papers still being published regularly now (Furnell 2022a; Lee, Sjöberg and Narayanan 2022)) — they also came up in Chapter 4, in many similar ways as will be reflected below. The ubiquity of this security method — both in general as well as in the potential measures that families suggested they would try to improve — as well as the acceptance that people do them poorly warrants special attention here.

In total, seven of the families ended the game and subsequently discussed methods of creation and use of passwords that were at odds with that of the current advice of the NCSC.[4] Many families found that, in amongst their various places of work and school, they had to adhere to different requirements about password creation and length of time for using them. One participant, who had worked in enterprise-level cyber security for a number of years, pointed out that, actually, organisational preferences for password management will likely be different to individual password management best practice. Organisations must work on the basis that their employees are not good at password management, and so will reuse passwords, ending up at the point of needing frequent password changes to lessen the risks coming out of a data breach. But this, arguably, goes on to embed poor password management in personal practice, even where it might be easier to do otherwise. *"I've got children with a reading age of less than five [in the class that they teach]. So try to get them to come up with a password that's got numbers, symbols, capital letters...what happens is they write it down."* (R2O2AF).

Four families — or more specifically, one member of each of these families — had encountered the idea of using longer passphrases, in line with the idea of the NCSC's three random words campaign. This campaign was referenced in one of the Quiz questions (as shown in Figure 17b), but in instances in the post-game interview where a family offered an answer of a strong password involving a version

[4] In particular the guidance around using three random words as a means of creating strong, unique passwords.

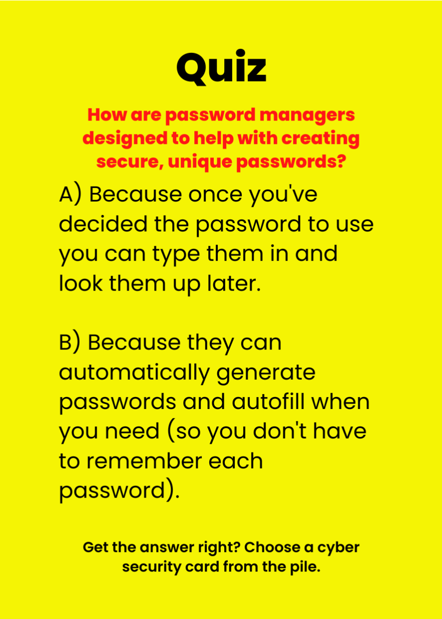
of *"letters, symbols and so on"* (R3O4C1, aged 15), they had not encountered the question.[5]

R1K3C2, aged 10, mentioned that they had known about three random words because of an advert on the radio that had stuck in their head. The remaining members of their family went on to point out that — even with the three random words idea — there were just far too many passwords to keep track of.

> R1K3C2, aged 10: *You're also supposed to have lots of different passwords for different things.*
>
> R1K3AF: *Yeah, that's not realistic though, is it?*
>
> R1K3C1, aged 12: *I'm not going to have 200 different passwords for 200 things!*
>
> R1K3C2: *Yeah, but that's what's recommended!*
>
> R1K3AF: *But you know, how often do we do what's recommended? Who does all that exercising? Who doesn't eat too much sugar?*
> R1K3C2: *But like you have the label on with the grams of sugar...*
>
> AF: *Yeah, but you skip that information because it doesn't really mean much.*

Despite recognition that *"it's hard to have passwords for ten different things"* (R1L9AF), very few participants actively used password managers. The most common finding was that adults had used password managers for work purposes, but found them cumbersome to use, much the same as in Chapter 4. Other participants were unclear what they were, or why they might be beneficial, or whether it was safe to use in-browser managers. As with the idea of three random words, participants that encountered the Quiz question that asked what a password manager did not subsequently display this uncertainty (see Figure 32 for the Quiz question on password managers).

[5] In these instances, the researcher then prompted the families to go and try the Quiz question.



Quiz

How are password managers designed to help with creating secure, unique passwords?

A) Because once you've decided the password to use you can type them in and look them up later.

B) Because they can automatically generate passwords and autofill when you need (so you don't have to remember each password).

Get the answer right? Choose a cyber security card from the pile.

Figure 32: Quiz question on password managers

As such, although by the final version of the game, there were Quiz questions about both password strength, password managers, a square on the board directly linking data loss to poor passwords, and threat cards where players would be penalised for not having strong passwords, it still seems to remain the case that passwords are both something that people know they must use, whilst also not having the understanding of how to use them in the most efficient and effective way.

Family discussion

As mentioned above, ongoing family discussion was reported as being the most frequently implemented cyber security measure after a week had passed, in keeping with findings from prior research (Ko et al. 2015; Blum-Ross and Livingstone 2020), and with the main goal of the game itself as a primary means of evidencing the awareness-raising ability of the game. It is worth taking some time, however, to consider what family discussion looked like during the gameplay process to understand what good discussion looks like, and also what types of discussions came up.

One important aspect of discussion in the gameplay process itself was where some, or all, of the participants had a lack of knowledge — whether they were aware of this lack of knowledge or not. Some parents discussed how, perhaps despite appearances, there were obvious gaps in their children's knowledge: *"[they] are just not very savvy, though. Like, they don't understand the concept of mobile data. Because the Internet's just there..."* (R1F1AF). R1F1AF, a teacher, also went on to discuss the children in her class (aged around 10 years old): *"I think [they] are so confident they can have incorrect assumptions, for instance one said 'I think 1234 is a good password because no one would believe you'd use it.'."* One participant, writing in the feedback survey, commented: *"...my children seemed very aware of not talking to strangers on the Internet and the risks around that, but they didn't seem to remember being taught about cyber security in any sense. I'm not sure what our school is teaching on this front, so I've emailed to ask out of interest. Whereas I know that it's very important that children know the dangers of talking to strangers on the Internet, it feels like cyber security is just as much of a risk and my children didn't seem to know anything about it"* (R3O10). Other families pointed out that children do not necessarily get exposure to the types of technologies that come with higher levels of security by default. Most adult participants, for example, had encountered some form of two-factor authentication in relation to online banking, an activity that most children will be too young to engage with.

Children do occupy an unusual space when it comes to their use of technology. Whilst, of course, the examples above show a lack of lived experience or appropriate reasoning skills, perhaps, in other ways, some children have skills far beyond their parents. Although this does not necessarily map over directly to home IoT device security, children could explain about how and why they circumvented barriers to accessing the Internet or devices directly:

> R3O7AF: *Anything else we can do to help keep our devices safer?*
>
> R3O7C3, aged 14:*Use a VPN?*
>
> Researcher: *Do VPNs help with devices?*
>
> R3O7C2, aged 14: *No. Basically what it allows you to do is if it creates a tunnel to the Internet that stops people from seeing how you use it. But then you can also change locations – so if anyone would track you later on, they wouldn't know where you are.*

> R3O7AF: *Do you try and use VPNs to get around family controls?*
>
> R3O7C1, aged 18: *It doesn't really work for that. It's more, it's more about getting access to websites. You can't get around Screen Time.*

Parental controls also are a blunt instrument, particularly as children grow:

> R3O4AF: *I thought I'd get Family Link to limit the amount of time they're on the phone, I've got Family Safe...but they know how to get around it!*
>
> Researcher: *And why, R3O4C1, aged 15 and R3O4C2, aged 12, do you try and get around the measures?*
>
> R3O4C1: *"Well, R3O4AF's not always here, and if they're not, then I can't [access the Internet because of the parental controls].*
>
> R3O4AF: *If C1, aged 15, comes home, and I'm still at work, why wait for me? Because obviously I can't do anything for the Internet [when I'm at work]. The [difficult thing] is trying to find a way that it works for all of us. I find that quite hard.*

This mismatch, which could be described as a mix of a lack of wider-world awareness, coupled with technical capabilities in some specific instances, underlines the importance of parents leading the way in trying to combine the two. However, the ability to inform children relies on two main aspects: the conversation has to be able to happen, and the person leading the conversation has to have the right information to hand — and the confidence to impart it. On the first: it was noticeable how many parents commented that it was unlikely that this conversation would ever happen in the normal day-to-day:

> R1L10AF: *Family discussion...what is that?*
>
> Researcher: *Well, it's just talking. Talking about the rules of what you want to do with technology.*

> R1L10AF: *Nobody talks about that! Well, that's the reality. Nobody knows.*

Another participating family wrote in their feedback survey that they could not *"believe we haven't talked about this before"* (R2O1), with other families recognising that children simply may not want to have that discussion: *"It was a great opportunity to talk about digital safety without actually forcing the children to have a conversation."* (R3O4). The game helped facilitate conversations that would not otherwise naturally, or easily, have occurred.

All families, as part of the gameplay kit, were provided with the guide to what some of the terms of in game meant. Many families either did not notice it, or use it during the game: only two families decided to take it home to further conversations at home, although many more recognised the need to *"discuss what [terms] are"* (R2L6AF) as part of the game. One participant, R2K1AM, decided to take it home as *"...you have to have [definitions of] certain words. And that's the discussion [you have to have]. C1, aged 14 is reading the authenticator app card. So we have to say, 'Oh, do you know what that is?' It's this discussion; you probably need to have an adult or a knowledgeable person being able to say what does that mean?"*. Sometimes the words themselves were a problem. In a sign of the privatisation of security measures, one participant, R1L7AF, did not know the term "authenticator app", but when the researcher began to explain, they asked *"oh, is that, like, Duo?"*[6] — a specific authenticator app. The privatisation of security measures not only adds costs, but it also makes it harder to discuss measures generically.

When family members could explain, there were good examples of knowledge sharing, between both parents...

> R3O9AF: *What's password manager because I've not come across that?*

> R3O9AM: *When you sign up to a website, and it says to create a password, sometimes you get an option to use Password Manager. And it will come up with a completely random [password] literally just a mixture of letters and numbers.*

[6] `https://duo.com/`

...and parents and children:

> R2O2C1, aged 14: *I think automatic software updates... I've never come across it. [Why] would it need to be in place?*

> R2O2AM: *Because it affects security. So there's lots of cases where large organisations have that built into [their] laptops. [When vulnerabilities are found] they have to do a big update.*

Yet, far more common was a lack of confidence or understanding in parents, meaning that they themselves either could not explain a coherent course of action, did not completely understand it or did not consider the action important or valuable. At the time of playing the second round of the game, Apple had asked users to download a software patch in order to fix two zero-day vulnerabilities (Abrams 2022). Most participants had heard this news, and some had actively looked to fix it.

> R2K1C2, aged 13: *I didn't get the notification to update, so I went and found it myself.*

> R2K1AM: *But then sometimes when you do get information like that, you need to think — am I getting this from a trusted source?*

The cynicism and mistrust around updates — one of the clearest ways of keeping a device secure, on the whole — was shared by both adults and children. As with R2K1AM, other participants were aware of being *"constant[ly] barraged"* (R1L7AM) with e-mails and notifications leading to confusion as to what was reasonable to believe. Children had stories of their smartphones (typically older models) stopping working after security updates: *"...that is how my [smartphone] died because it couldn't process a security update. And then the entire thing malfunctions, and partly because of that it might put you off [doing it again]."* (R3O7C3, aged 14). Parents also struggled with the nuance required to explain to children that some notifications, buttons or links must not be pressed (whether to avoid phishing, or inadvertently buying something), yet that updates should be done — despite both of those actions feeling very similar. Issues like this are not easily sorted through gameplay alone, although anything — such as the

Table 27: Participant and control outcomes

(a) Participant outcomes

	Round one		Round two		Round three	
	Yes	No	Yes	No	Yes	No
Purchased new device	0	9	1	9	0	10
Received training	1	8	2	8	2	8
Saw news articles	1	8	2	8	3	7
New cyber security measures	7	2	7	3	7	3

(b) Control outcomes

	Round one		Round two		Round three	
	Yes	No	Yes	No	Yes	No
Purchased new device	21	94	10	87	12	85
Received training	16	99	9	88	8	89
Saw news articles	23	92	26	71	6	91
New cyber security measures	9	106	6	91	6	91

terminology book — that arms participants with knowledge and some confidence may help support trickier conversations.

In terms of RQ4b — "Do families understand a wider range of threats and risks of using home IoT devices after playing the board game?" — it would seem that playing any version of the game did help raise awareness, with the third version of the game perhaps been most beneficial. Repeated playing may help, too. However, issues around passwords and having the right knowledge to facilitate accurate discussion remains problematic.

Game Results compared to the Control Group

We have seen in the previous section that 21 of the 30 gameplaying sessions resulted in at least one known cyber security change a week later (see Table 26). In order to try to understand a bit more clearly whether or not these changes were likely prompted by the gameplay or by other events happening in at the time, for each round of gameplay, a control survey was undertaken, as described in Section 6.2.4. The possible difficulties of using differently sized participant and control groups is considered in Chapter 6. These questions were also asked of the participants filling in the feedback survey the week after gameplay. The overview of the results can be found in Table 27.

What can be understood from a chi-squared analysis of the results,[7] is that the

[7] As mentioned in Section 6.2.4 and Chapter 6 given the small number of participants in each

gameplay groups were statistically significantly more likely to have made changes to their cyber security measures than the control group — no matter which round of gameplay: round one: $\chi^2(1, N = 124) = 36.34$, $p < .001$; both round two: $\chi^2(1, N = 107) = 31.36$, $p < .001$; and round three: $\chi^2(1, N = 107) = 31.36$, $p < .001$. Both groups were asked about whether they had bought new devices (that might come with instructions) or received any cyber security training in the period before answering the survey: the chi-squared analysis showed no statistically significant answers, suggesting that these aspects should not have been a factor in the higher number of changes made by the gameplay group (had they received a higher amount of training or bought a larger number of devices, it could be argued that these may have also had a bearing on the changes made). The surveys also asked whether the respondent had taken notice of any technology news in the period before the survey. Rounds one and two had non-statistically significant answers, but in round three, more participants from the gameplay group reported noticing the news than may have been expected ($\chi^2(1, N = 107) = 6.67$, $p = .01$). Further investigation into the news being reported by the gameplaying families confirmed that they were not directly cyber security related,[8] suggesting, perhaps, that the families had been more observant of technology news than might have been expected (although, it is, of course, noted that the stories mentioned were, at the time, large news events — although it was not reflected in the control group survey despite both surveys occurring at the same time).

The results from the analysis of the non-control and control group shows that the answer to RQ4c — “Do participant families make changes in the cyber security methods they use at home in the period after playing the game?” — is yes, in comparison with the actions of the control group.

round of the gameplay, and different sizes of control and participant groups, using statistical methods of analysis may be considered questionable, but have been used as a means of trying to show the comparison between gameplay and control groups.

[8] The news items reported were the takeover of Twitter by Elon Musk, by two families, as well as reporting into a Bitcoin scam, and a report about the tapping of UK politicians’ smart phones.

7.2 Discussion

This section will consider some of the findings of the game and their implications. In particular, the discussion will consider first whether the entire game experience worked to provide answers to RQ4, and will detail out the new *RFs* generated from the research.

Did the game work to provide answers to the RQ?

The game hoped to explore RQ4 — how can a board game act as an intervention to support participant families to improve awareness in relation to the cyber security of home IoT devices that they own and use? Could the game positively serve as an opportunity to provide training and education to provide the awareness needed to move participant families from a state of precontemplation on the TTM cycle to one of contemplation or beyond? Also, more negatively, could it show which aspects of cyber security for home IoT devices seemed beyond the reach of the participating families?

All the previous RFs (1–10) showed that understanding — and the ability to begin to find knowledge and learn in order to have discussions and put good practice into action — is difficult, if not impossible, for the average uninterested family to achieve. This means that the majority of families will need awareness, which is bolstered through training and education, to move forward in any cyber security journey. Therefore, helping to bolster knowledge learning and discussion within the family was the key starting point when considering how to support the user, in trying to create an intervention that might work, or in understanding what was just too complicated to take further. As such, the approach of a game was, in part, a way of considering this question; the role of UCD was perhaps a more indirect approach. But, as the researcher is far from a board game designer, this step felt significant to create a game that felt enjoyable, not just passing on knowledge. That said, the outcome of three rounds of design with families was a board game that scored very highly not only for enjoyment, but also on feelings about whether or not the participating families learned about both device use and cyber security. It is important to recognise, too, that the content of the cyber security knowledge in the game did not change throughout the rounds — there were modifications to the delivery (particularly in the case of the Cyber Security

Battle and the introduction of more devices), but the core aspects of learning did not change. That the game became more enjoyable and also made families feel like they were learning more hopefully means that the final version of the game was a better educational tool, made so as a result of the improvement in design.

In showing that participants could name a broader range of threat types, more specifically useful types of cyber security measures, and ultimately, in making changes to the cyber security measures in their homes, the game seems like it has been a successful intervention in giving a training and education opportunity that showed evidence of awareness raising (through discussion) if not motivation to action in the following week — particularly when compared against the control group. That the most changed cyber security measure was discussion, suggests the game has been successful in bringing families — both nuclear and wider, as well as friends, in some cases — to a better place of awareness at least.

Yet, still, nine participating families made no known changes. This is still a vastly smaller number than the participants in the control group that made no changes, and in at least one case was because of existing expert knowledge, but still a relatively high figure. This suggests there remains difficulty, complacency or a lack of impetus to make changes in many cases. What else might be needed to continue to improve understanding and, in theory at least, reduce the number of families not taking any steps further, or mitigate this inaction?

7.2.1 Research Findings

This section will list out the *RFs* from the two aspects of the game research: the UCD and cyber security awareness elements.

User-centred design

***RF 11:* Working with families created incrementally more enjoyable versions of the game that families felt they learned more from**

The feedback survey indicated that each version of the game was more enjoyable than the last, and made participants feel like they learned more, and had more of an opportunity for discussion, as well.

RF 12: Nuance had to be removed to make for a more engaging experience

In particular, game mechanics about data flows, providing information on game cards and the introduction of winning helped to improve enjoyment ratings — whilst seemingly not impacting knowledge transfer and family discussion.

RF 13: Competitive gameplay is extremely popular

However, any type of gameplay is only valuable if they are covered in the game — the chance nature of gameplay is such that not all cards were used in the game, leaving areas of knowledge untouched, based upon one round of gameplay, in many cases.

Cyber security awareness

RF 14: Scenarios seem to help broaden awareness

The use of Inside and Outside Threat card within the games, having, as they did, small scenarios for teams to consider, seems to have broadened the awareness of participants (immediately after the game at least) around the types of threats that they might face as part of device ownership. Interestingly, however, device manufacturers were not considered by any families as a threat before or after the game — despite appearing in three Outside Threat scenarios in different guises, suggesting that there may still be gaps in mental models when it comes to how home IoT devices work.

RF 15: Understanding data — particularly in relation to money — remains extremely hard

Throughout the gameplay sessions, participants found it hard to conceptualise data, and the importance of the loss of data. In comparison, participants could — and did — easily understand the value of the money. Although it is valuable that participants began to understand the inherent costs of device ownership beyond their privacy, the value of the money within gameplay was typically overstated by participants.

RF 16: There seem to be pros and cons of playing online and playing face-to-face in a controlled setting

Although it is hard to draw definite conclusions based upon the small numbers of participants for each round, online participants seem to have made more changes, overall, and this might be because they were playing in the context (the home) in which changes were to be made. That said, offline participants seemed to take in more about the types of threats that could befall them — possibly this is something to do with feeling more comfortable to think of "bad things" happening out of the home setting.

RF 17: Playing more than once may be beneficial

Again, it is hard to draw firm conclusions based upon small numbers of participants, but it did seem, based upon the numbers of changes made, that playing the game more than once conferred a benefit in terms of allowing for further consideration of cyber security measures in the home, thus giving participants a second chance to reflect and make changes.

RF 18: All versions of the game were better than doing nothing

The control group showed that playing the game made it significantly more likely for a participant to make changes to their cyber security measures in the home.

RF 19: Discussion needs a prompt to start, but needs knowledge to continue

Families were most likely to report having had discussions about cyber security in the week following gameplay, but even the ability to play the game helped as a starter for conversations that were difficult to have or that children appeared resistant to. Parents recognised, however, that these conversations were harder to have when they did not feel they had the knowledge themselves.

RF 20: Passwords remain a perpetual issue

As seen in the questionnaires and feedback surveys, as well as in conversation with the participants, it is known that passwords should be strong and unique.

It seems to be accepted, however, that this is too hard to achieve, and so people do not do it. It is made worse by inconsistent password requirements in different strands of people's lives.

***RF 21:* Other cyber security measures remain hard**

Although participants did make a range of changes, these were accompanied by a number of problems, from implementation to understanding. Participants also discussed the difficulty of finding measures that suited all family members — with children being quite open about the fact that these measures were typically imposed upon them, making it necessary to find workarounds to do what they would want to do.

7.3 Limitations

The major limitation of the structure of the research links to the number of participant families involved in participation. As mentioned in Chapter 6, a relatively small number of participant families was inevitable and planned for, given resource constraints. However, this number constrains the ability to perform meaningful statistical evaluation of the results. This is doubly so in the case of the control group — the difference in size between participant and control groups makes for arguably dubious evaluative statistical analysis. As such, the comparisons made should be considered more descriptive than statistically rigorous in nature, although the consistency of the results should act as some comfort as to the usefulness of the cyber security findings.

A second major limitation of the research method is the lack of time available to do a thorough ongoing review of actions taken by participant families. This is frustrating, as understanding the long-term aspects of TTM — whether users continue maintaining their security measures or whether they relapse into not using it — could be extremely useful when considering recommendations about specific cyber security product use.

Finally, the game gave no particular weighting to any one cyber security measure, rather allowing participant families to explore a range of measures without guidance. This meant that in some cases, measures may have been decided upon with an inappropriate or incomplete basis of understanding (particularly as so few families interacted with the explanation booklet) — given the generality of some of the measures (e.g. anti-virus software), it may be that the game provided too wide a range of options, with the downside being that the most effective measures were not necessarily chosen, or fully understood as such. In addition to this, with cyber security methods often being subjective in their use, it could be that the representation of the measures chosen was not the most objectively appropriate for participant families. With more time and resources, it may have been possible to improve the objectivity around the usefulness of particular cyber security measures through using a Delphi study, for example. However, in the event, given the starting point of so many of the participant families (at a place of precontemplation), it was considered that any awareness raising would be beneficial, even if nuances of description or surrounding use could have been further refined.

7.4 Conclusion

This chapter has recounted the findings from the final piece of research in this thesis, which addresses RQ4 — how can a board game act as an intervention to support participant families to improve awareness in relation to the cyber security of home IoT devices that they own and use?, building on the previous pieces of research detailed out in Chapters 4 and 5. The process of the research was broken down into two main aspects: the UCD of a serious game that families could play to further their knowledge together about the cyber security of home IoT devices, and whether or not that game did, in fact,provide training and education that could at least raise awareness, and possibly engender action in some cases. The intention with the use of a serious game was, in part, to see if it could act as an intervention in and of itself; it also allowed for an immersive experience for families that could show which aspects relating to the threats or cyber security measures brought up in the game did not land well with the families playing it. It was thought that where this happened, it might make a case for interventions occurring elsewhere — perhaps changes needing to be made by manufacturers, or at a policy-level.

The first round of the UCD process started with a game designed by the researcher, and piloted in the University department. Throughout the rounds that followed, the key learning elements incorporated into the game — the types of threats, potential cyber security measures,[9] the loss of data as well as money — remained the same, albeit delivered in different ways as the rounds progressed. As the rounds progressed, elements were included to improve engagement, through a combination of more competitive gameplay, clearer playing materials, and the removal of more complex game flow. By the third round, the families consistently rated the game as more enjoyable, with better opportunities to discuss and learn about cyber security as a family. This suggests that the improvement in gameplay added to the game's ability to raise awareness, if only through more discussion that would otherwise not have been held. This is important as those families had not seen or played any of the previous iterations of the game, suggesting that the UCD process had worked to create a more enjoyable game.

The game seems to have helped in moving participant families around the TTM cycle, whether just by starting the discussion as a family or even moving to make changes to their cyber security setup at home. Participants, in all rounds, were able to report a wider range of threat types immediately after playing the game, and displayed a more nuanced understanding of the types of cyber security measure more applicable to home IoT devices than immediately before the game.

Participants also reported making changes (moving through the TTM stage of "action") based upon things they had discovered in the game; significantly more than those in the control group. A number of families suggested that the primary thing that the game prompted was more discussion, with the understanding that this discussion simply would not have happened otherwise. It is interesting to note, however, that there seemed to be a slight preference for one-time-action measures (guest networks, changing router passwords) — when they worked immediately. Longer-term measures either were not changed (notably password management), or started to grate within the week of the intention being noted (such as was the case with unplugging devices when not in use). Although not considered in depth in this work, this has important implications for the relapse/maintenance stage of TTM.

As such, it seems that the game, in and of itself, did work well as a measure of training and education leading to awareness raising, particularly by the final round. It highlighted areas that may need intervention from elsewhere, too: discussion within the family is excellent, but it needs to be based upon evidence,

[9] With one measure removed as it caused confusion.

which often is hard. Passwords remain extremely complex, and other measures remain far from easy, often with less than perfect results. It is with these conclusions that we now turn to the final chapter of the thesis, to review what the research has found, and what the implications of this must be for families, industry participants, academics and policymakers alike.

Chapter 8

Conclusions

This final chapter will provide a brief overview of the thesis as a whole, restating the reasons for, and findings in relation to, each RQ. It will move on to reflect upon these findings holistically, and then provide a number of recommendations for various stakeholders.

8.1 Overview of thesis

At the start of the thesis, a literature review (undertaken in January 2020) found that there were many aspects in relation to families' use of home IoT devices, and wider understanding of cyber security that had not been directly considered. It pointed to significant consideration having been given — for adults, parents and children individually — in relation to online harms, and how the family might discuss threats like stranger danger or oversharing online. Perhaps because of the relatively nascent nature of home IoT devices, literature about how families — as opposed to any group, regardless of the composition — use these devices was not prevalent at all: neither was literature focussing upon the understanding of cyber security, rather than just the privacy concerns that such devices may pose.

As such, four RQs were posed, which will be set out and discussed below.

8.1.1 Overview of RQ findings

Having performed the literature review of this thesis, the following RQs were posed:

RQ1: What is the level of awareness exhibited by interviewed and surveyed families in the UK in relation to the cyber security of home IoT devices that they own and use?

RQ2: What knowledge is available online to those who wish to implement cyber security measures for home IoT devices?

RQ3: How can a researcher effectively understand and act upon the lack of awareness and motivation to consider the cyber security of home IoT devices shown by families?

RQ4: How can a board game act as an intervention to support participant families to improve awareness in relation to the cyber security of home IoT devices that they own and use?

These RQs were mapped onto the work undertaken in Chapters 4, 5, and 6. The overview of all *RFs* can be found in Table 28.

8.1.2 Use of the Transtheoretical Model of Behaviour Change

This work was considered in light of the TTM theory, as framed by Faklaris, Dabbish and Hong (2018) for cyber security adoption. The use of the model helps reflect the journey that individuals need to go on to get to a place of robust cyber security that is appropriate for them, a really important part of understanding how to support behaviour change. The initial assumption, which the research in Chapter 4 showed, was that many families were in a state of precontemplation, the very first step of the cycle, roughly equivalent to not even recognising that there was a problem that may need to be solved. The following two pieces of research helped to explore, first, what sorts of information was accessible — and if it was sufficiently relevant to be used as a training or educational tool, and second, what gaps could stop any sort of awareness being raised within the home. The final piece of research used this information to create a game that provided a variety of ways for families to learn about cyber security as it could pertain to home IoT devices, with the idea that the level of training and the method of a competitive board game face-to-face could help raise awareness. Awareness raising, in the TTM model, is a key action to move to contemplation: should we use cyber security measures? In the game, it was considered that discussion among family participants was a way of showing that the stage of contemplation had been reached. In some cases, the game moved many families further still around the cycle, through preparation to action — actually making a change in their home IoT device security setup. The research did not take place over a long enough period of time to consider the final stages of the cycle, either relapse (into inactivity) or maintenance of security use, although there was suggestion from those families that had made a cyber security change that single-action changes were much more easily maintained, than those requiring ongoing work, even after only a week.

8.1.3 RQ1:What is the level of awareness exhibited by interviewed and surveyed families in the UK in relation to the cyber security of home IoT devices that they own and use?

For RQ1, families were interviewed and surveyed. Despite being relatively keen to have devices in the home, families did not have a clear understanding of the threats and potential risks that these devices could pose. This lack of understanding comes from the relative novelty of the devices: with neither adults nor children having an opportunity to be taught, formally or informally, about these devices, many participants could not understand how they might pose a problem, beyond potential financial fraud. Participants were happy issues of financial fraud could be resolved through working with their financial institutions, even though this may not be the case. When asked, families reported that they discussed issues of online safety significantly more frequently than even the most basic of cyber security measures, and any such measures would be those applicable to using computers, rather than home IoT devices. Even if there is overlap with the security measures discussed, they were never discussed in relation to the devices. In addition, rather than being concerned about cyber security issues, almost all parents explored, directly or indirectly, how they promoted careful use of the devices to the children, given the expense of replacing them — potentially introducing further cyber security risks into the home as a result.

The answer that must be given for RQ1, based upon these findings, is that families do not discuss the cyber security of home IoT devices at present; any management done is not discussed or necessarily holistically considered in most families. In terms of the TTM model, participant families mostly seemed to be at the precontemplative step (as assumed at the start of the research); further training and education would be needed to provide the awareness needed to move further around the cycle. Why is it that the existing method of support — searching for the answers online — did not work as a training or education method, and what in the home setting could prevent exacerbate problems around implementing cyber security for IoT devices?

8.1.4 RQ2: What knowledge is available online to those who wish to implement cyber security measures for home IoT devices? and RQ3: How can a researcher effectively understand and act upon the lack of awareness and motivation to consider the cyber security of home IoT devices shown by families?

Two pieces of research were undertaken to consider different aspects of RQ2 and 3. The cyber security information review was undertaken, given the finding coming out of the interviews and surveys that the Internet is the main source of solutions, should issues occur with devices. Yet, the information that is available is too general to be useful without the user having given some real thought as to the threats that may affect them, and having some understanding of what credible guidance may well be; both of which seem unlikely to be able to happen, based upon the interviews and surveys. This is an active hindrance in terms of appropriate and credible awareness raising.

The second piece of research covering this RQ was the autoethnographic diary study. This piece of work, performed by the researcher about her own experiences, found that cyber security rarely arises in everyday use, and so the ability to discuss it is infrequent — even in an interested and informed household. When these issues do come up, there are language issues immediately — how do you describe how things work, or what cyber security measures are to young children or older adults who do not have the language (or interest)? Setting devices up to be privacy-preserving and, in theory, with slightly higher levels of security, may cause devices which are hungry for data and constant Internet access to work poorly. Should cyber security issues arise, knowing about cyber security in general may not be any help when faced with solving a real-life cyber security concern, again explaining the state of precontemplation that so many families are currently in.

The answer that must be given for RQs 2 and 3, based upon these findings, is that there are several issues that families may encounter when trying to manage the cyber security of home devices. As a start, and as considered in RQ1, they may not have the information to manage devices securely to start with, and simply not know where to find it — or be able to find it at all. Should they look online, they will find a myriad of opinions with little to no specific guidance. Should steps be taken to make devices more secure, the devices may not work properly. And discussing cyber security remains incredibly hard, making the idea that it would become something that families can discuss together extremely unlikely.

8.1.5 RQ4: How can a board game act as an intervention to support participant families to improve awareness in relation to the cyber security of home IoT devices that they own and use?

Building upon the findings for RQs 1, 2 and 3, it was recognised that to start understanding what types of interventions would be needed, the research to do so would require the immersion of families into the subject, as passive observation would likely be insufficient to draw conclusions. As such, the decision was taken to create a board game, which could be tested as an intervention in its own right by providing training and education that could raise awareness, but that could also point out areas where more significant interventions by other stakeholders may need to be undertaken.

The board game, which was designed with participant families, created a game that was enjoyable, and as the rounds progressed, allowed for discussion and immediate expansion of knowledge in relation to what may be a threat and what type of cyber security measures may be helpful — that is to say, increasing awareness by providing meaningful and engaging training and educational examples. It also seems that the game inspired participants to alter their home security setup (moving through to the "action" step of the TTM cycle), when compared to a control group. Almost all participant families engaged in discussion during and, in some cases, after the gameplay session. With discussion being a reasonable indicator of awareness sharing, the game could be said to be an awareness-raising tool for families in its own right.

Despite this positive outcome, the gameplay still showed areas where families could not do or understand the secure thing, even where the will was there. Within gameplay, numerous families, at every round, questioned the importance of the representation of data, relative to the money in the game — with children particularly keen to play with the money, but not being concerned about the data. In particular, and echoing the findings in the previous RQs, although some participants made changes to specific aspects of their home network, for example, this remained trial and error, to a degree, with at least one family being unable to figure out how to make the intended measure work. Other aspects that required long-term effort on the part of the participants had, in some cases, already become a test of willpower within a week. Finally, as is well known, passwords remain extremely hard for users, and despite being aware of this, the effort it takes seems to outweigh the perceived benefit.

The answer that must be given for RQ4, based upon these findings, is that a board game, such as the one created here, was shown to be able to act as an intervention, as it allowed participants to immerse themselves in an experience close to their own, but not real life. As they played, they were able to discuss things as a family (showing "cognition"), and start to apply the concepts to their own lives (showing "action"). Whilst this intervention acted as intended, participants still showed a number of ways in which they would need support, meaning that other complementary interventions remain necessary. These additional interventions could range from improving security options and settings provided as standard within home IoT devices, to ongoing support and explanation of best practice cyber security measures from manufacturers and governmental organisations and enhanced curricula to embed a security mindset for children at an early age.

Having laid out the findings as they relate to the RQs, overarching points relating to these findings will now be discussed.

Table 28: Research findings

Research Finding Number	Research Finding	From which piece of research
1	Families are happy to use devices, particularly Smart TVs and Smart Home Assistants, without proactively considering security	Interviews and surveys (Chapter 4)
2	Families do not have a clear understanding of the threats and risks their devices may pose	Interviews and surveys (Chapter 4)
3	There is a lack of opportunities for learning for both adults and children	Interviews and surveys (Chapter 4)
4	Parents model behaviour promoting careful use of devices, the importance of saving money and understanding consumer protection frameworks — but not security	Interviews and surveys (Chapter 4)
5	Users need to understand what is a threat to them specifically to apply any cyber security information they might find	Cyber security awareness information review (Chapter 5.2)
6	Information about device security likely needs wider context to be accurately applied	Cyber security awareness information review (Chapter 5.2)

Continued on next page

Research Finding Number	Research Finding	From which piece of research
7	Hard to find credible guidance	Cyber security awareness information review (Chapter 5.2)
8	Cyber security rarely arises in everyday device use	Autoethnographic diary study (Chapter 5.3)
9	Solving cyber security issues can be uncomfortable and hard	Autoethnographic diary study (Chapter 5.3)
10	The language of cyber security is too complex for day to day interactions with non-experts	Autoethnographic diary study (Chapter 5.3)
11	Working with families created incrementally more enjoyable versions of the game, that families felt they learned more from	Game research (Chapter 6)
12	Nuance removed had to be removed to make for a more engaging experience	Game research (Chapter 6)
13	Competitive gameplay is extremely popular	Game research (Chapter 6)
14	Scenarios seem to help broaden awareness	Game research (Chapter 6)
15	Understanding data — particularly in relation to money — remains extremely hard	Game research (Chapter 6)
16	There seem to be pros and cons of playing online and playing face-to-face in a controlled setting	Game research (Chapter 6)

Continued on next page

Research Finding Number	Research Finding	From which piece of research
17	Playing more than once may be beneficial	Game research (Chapter 6)
18	All versions of the game were better than doing nothing	Game research (Chapter 6)
19	Discussion needs a prompt to start, but needs knowledge to continue	Game research (Chapter 6)
20	Passwords remain a perpetual issue	Game research (Chapter 6)
21	Other cyber security measures remain hard	Game research (Chapter 6)

8.2 Final discussion

8.2.1 How are families supposed to know what they are buying into?

The interviews showed that people like the novelty — and sometimes, the practicality — of home IoT devices. This possibly arises from a combination of things: such devices tend to be marketed well — and, in the case of devices such as the Amazon Echo, can be deeply discounted during sales periods — or slowly become the only option (as is becoming the case with smart TVs and white goods). As the interviewees (and the autoethnographic diary study) made clear, too, there can be benefits from these devices too — starting to remove household burdens, to help people feel safer in their homes, give access to things (such as books) that may not otherwise be so easily available, or just feeling more comfortable.

The issue that home IoT devices users face today is that **understanding the longer-term implications of using the devices is too uncertain and complicated.** The game showed that people still cannot conceptualise, and do not worry about, the data that they provide to these devices. They are also provided with minimal information to be able to explore what cyber security might need to look like for their family for each device, or cumulatively for their entire home network. And this may lead users to be providing data to services where they do not fully understand the purpose (or the possible end use) of the data that is being collected: as an example, Amazon have recently scaled back the teams that work on Alexa/Echo. Amadeo (2022) reported that the selling of the Echo devices more or less at cost (to make them enticing) is too expensive for the company, and users do not use them as intended, meaning that the stated business model relating to Alexa/Echo "...to make money when people use our devices, not when they buy our devices" fails. Amazon's goal was that people would use their devices as a frictionless gateway to buy things. What seems to be happening, however, is that this is not happening — but users will still provide data to Amazon, and may still carry various risks from using the device. We have seen similar extensions of purpose reported about the Ring doorbell systems, where data has been provided to police without the user's knowledge (Ng 2022).

These examples may not explicitly focus on the cyber security failings of these products, but they speak to the **difficulty of trying to secure devices — which in many cases may mean providing less data — when it is difficult to understand precisely what the device may be trying to do, not just for the user, but also for the manufacturer.** The interests of manufacturer and user are not aligned when it comes to security measures — the interviews and autoethnographic diary study highlighted this — devices typically have very short supported lives, and it is hard to know when that support stops. Should users try to turn off settings to share additional data, their service may be degraded as a result.

Without even a general knowledge, it is hard to take the next step of efficient threat management based upon personal situations. Extending the suggestions from Parkin et al. (2019) and Emami-Naeini et al. (2019a), **manufacturers must do more to make the key threats of home IoT device use clearer at point of setup, and periodically throughout device use.** Documentation about major threats relating to personal data and device misuse, and the recommended baseline steps to mitigate these issues based upon the specific device may help to increase awareness in adult users, which can, in turn, trickle down to children. Manufacturers may also focus on providing this information clearly online, so that when users are faced with trying to improve their knowledge, official sources are plentiful.

Home IoT devices — particularly those that must have a reasonable expectation of use by multiple people, indeed, multiple generations, within a single location — **should be provided with better guidance as to how to set them up for the situation it is located in.** Every person and every household has its own particular set of threats and risks that might make certain security options more or less appropriate for them; however, there will be certain baseline security features that should be promoted to users at the point of setup and periodically thereafter. Hiniker, Schoenebeck and Kientz (2016) and Ko et al. (2015) have shown that families are more likely to come to agreements over rules for Internet use if they agree upon these rules as a unit. Our findings agree with this: families instinctively use discussion as a means of managing potentially tricky areas for their children. However, previous research has shown children and adults may use different words to discuss cyber security (Jones et al. 2019). In addition, children may not perceive devices in the same way that adults do, not only, as our interviews showed, failing to understand they are connected to the Internet, but also in understanding how they work (Yip et al. 2019; Xu and Warschauer 2020). As such, the expectation that using discussion either to agree about home rules about home IoT devices or as a means of providing children with additional knowledge will fail, without further guidance for both parents and children.

8.2.2 Discussions need to be based on knowledge and understanding

A proactive family discussion about a topic is likely to be better than no discussion at all, as it suggests a level of awareness. It seems from the responses of the gameplaying participants that without the game, there would have been no discussion about cyber security in the home at all. However, the game showed the potential for the fragility of these discussions. As previously found in almost all the *RFs* from the prior pieces of research, there is no infrastructure in place to underpin these discussions. The game came with a guide (see Appendix P) with details about the terminology raised in the game. In many cases, participants, both adults and children, had a lack of understanding or some incorrect understanding — but reasonably held and based upon experience — about how best to go about implementing security measures. Even though this guide was also poorly used, the game gave visibility to cyber security measures that participants may not have given second thought to otherwise and — by the third round of gameplay — gave them the opportunity to get a feeling for what cyber security measures may be more, or less, useful for each type of device they own. They also had the opportunity to reflect, critically, on what the devices offered did, and whether they considered them worth the effort of the measures that they might need to implement to protect them. And even with these opportunities, real-life issues with implementation occurred.

Outside the gameplaying sessions, these opportunities for training and education leading to awareness raising, discussion and thought about implementation do not exist. This echoes the findings of the previous chapters, and remains a problem in the real world: how do we hope that parents can find the opportunity to learn about cyber security, and have the confidence to discuss it with their children? It can be seen in the gameplaying family with the expert parent that discussions about how to set up commonly agreed-upon cyber security measures at home can be done: that said, the findings of the autoethnographic research, and in particular *RFs 8-10*, show how difficult that can be without specialist knowledge, or with younger children or older family members who are not keen to learn.

In the UK, there is some expectation of support from the government for personal risk management. However, **the interviewees showed a complete lack of awareness of the existence of the body tasked with supporting them with cyber security, the NCSC**. There is an interesting case to be made for learning the public health messaging lessons deployed to spread messages around social distancing, and then the promotion of vaccination, in relation to COVID-19. Additionally, it is perhaps at this point that the usefulness of the scenarios created for the board game, or storytelling (Pfeffer et al. 2022), could be considered further. How can scenarios be woven into opportunities for cyber security awareness? At least one (child) participant remembered the three random words password radio campaign, precisely because the concept was clear and memorable. Teachers in the gameplay participants, and those that work with vulnerable people, also highlighted how much easier this concept would be to impart to those they work with. Threat scenarios, as used in the game, can be vivid without being wordy, and could form the basis of similar educational campaigns — both for adults, but also for children, in schools — from NCSC or equivalent government agencies. **The use of poster campaigns, short slogans and promotion of positive behaviour by government agencies and trusted members of society, whether in a personal capacity or through platforms, such as TV shows or recognised websites, may serve to normalise good cyber security measures.** This should sit on top of school-based education, and would serve to provide knowledge that is currently unavailable to both adults and children alike.

8.2.3 Appropriate levels of base security measures and explanations for home IoT devices

In addition to the ability to find and gather the knowledge, those deciding to make cyber security changes have to have the capacity to do it. In some cases, such as setting up guest networks, that may be technical understanding (or the confidence to try); in others, for instance, turning off devices when not in use or limiting settings, it may require habit changing or the introduction of precisely that sort of friction that the device was designed to minimise. It is also vital to mention that none of the measures suggested in the board game is a panacea in and of itself: a technical measure will help to mitigate a single technical problem. But discussion and lateral thinking is still required to implement a holistic set of security measures. As explored in Section 5.2, for example, you can set up a guest network, but what do you put on which network? How do you segregate devices if you need your smartphone to be on the same network to connect to your home IoT devices? There is no simple answer.

One group that was conspicuous in its absence, in terms of positive measures provided in Chapter 5.2, were ISPs. In the majority of cases, ISPs provide users with routers at the time of starting the contractual relationship for provision of broadband services. **ISPs, therefore, could play an enormous role in facilitating secure network setup, both at point of setup and by having prominent support sections on their websites.** On the basis that it is reasonable to assume that most houses have some home IoT devices, they should provide details on guest network options and how best to set it up, either to provide guests access or to segregate devices and computers, for example. Recent research has also found that ISPs can play a preventative — and much more targeted — role in stopping malware, either through ensuring more stringent technical measures for each user (such as closing unnecessarily open ports), quarantining affected networks and providing support directly to the customer to resolve the issue (Çetin et al. 2019; Noroozian et al. 2021). Additionally, ISPs should replace their customer's routers when they no longer receive appropriate security updates, a relatively simple process that could ensure significantly higher levels of security for longer-term customers.

Passwords remain problematic, as has been long considered (Morris and

Thompson 1979; Furnell 2022b; Taneski, Heričko and Brumen 2019). There is very little that the user can do in this situation. It has been discovered by Nicholson et al. (2018) that when users are instructed to create passwords that are longer, they have difficulty in recalling them — possibly because longer passwords introduce a greater likelihood of mistyping. Maybe password managers are a strong part of the solution, but again, this requires the willingness to use and also, potentially, a cost to do so — as well as having the ability to access the manager on any and all devices required, and trusting the provider to store your most sensitive data appropriately (Hay Newman 2022).

Calls to manufacturers and user alike have been to stop using passwords, if possible, in favour of biometric data, which is harder to hack, even if it arguably raises different data protection issues (Trotman 2021). This could be helpful when accessing home IoT device apps from a smartphone as a particular user. Some camera-based devices already have the options to use biometrics, but, help pages from Google's *Nest Aware* show[1] that the management of this is practically hard in the home: you may have to ask strangers if they consent to their biometric data being taken by your doorbell as they stand, for instance, at your front door; it cannot also not work for children under 13. MFA also feels complex for IoT device systems: purchases or other designated restricted activity could require users to click a link in an app, or read out a code sent through email or SMS, at a cost of the frictionless experience that the devices intend to create.

However, for any IoT device that requires app interaction to make changes to the device, such authentication becomes meaningless, as the authentication would be sent to on the same device as being used to make the changes. One alternative solution may be to require manufacturers to adhere to, and mandate the use of, the password guidance of the government in which they are operating (or the most secure of all the jurisdictions that they operate in). Chapter 5.2, backed up by findings in Lee, Sjöberg and Narayanan (2022), shows that this does not happen in practice.

The evidence from the interviews in particular suggests that **home IoT devices that are expected to be used by groups of people — especially children — should come with more stringent security measures set by**

[1] `https://support.google.com/googlenest/answer/9268625?hl=en`

default. For example, although some steps seem to have been taken by manufacturers to allow notifications when things are purchased, further work could make spending money and downloading items harder (requiring purchases to be confirmed with a PIN or other agreement from the primary account holder). Alternatively, a clear signpost to the potential risks of not protecting purchases at the point of setup, should be provided. The interviews show that, for example, adults in the UK are used to being protected by strong consumer protection measures that should cover most cases of fraud — but crucially, not "gross negligence" when, despite being the victims of fraud, they were deemed not to have taken the proper precautions (Brignall 2020). Although adult interview participants were extremely concerned about financial fraud, few had enabled settings to limit purchases on applicable home IoT devices, and no family considered the ease with which significant sums of money could be spent fraudulently, potentially without recourse.

It must be recognised that there are due to be measures brought in to mitigate some of the security aspects explored here, such as the UK's PSTI Act, mandating some aspects of security by design in consumer smart products, and ETSI's EN 303 645 baseline standard for consumer IoT (ETSI 2020). Much like the devices they seek to legislate and standardise, these measures are nascent, and may well need to be extended and revised as the market matures. It should be noted that the PSTI Act mandates a smaller subset of requirements, compared to the previous DCMS Code. Subsequent research performed by DCMS after the implementation of the Code found that even that wider range of measures did not do enough to protect consumers (Datta Burton et al. 2021). **Policymakers should continue to analyse the ongoing harms arising from the increased ubiquity of such devices to understand whether more regulation or legislation may be necessary to protect consumers and specific groups of vulnerable people in the future.**

An example of regulatory focus on a particularly vulnerable group would be the UK's Age Appropriate Design Code (AADC) (Information Commissioner's Office 2020a), which requires organisations to consider the safety of children explicitly, when providing those services within the UK. Acting unilaterally, as the UK government is in the case of the PSTI Act and AADC, works on the assumption that the measures can be applied to — and enforced against — those devices that are for sale in the UK in a meaningful manner, despite home IoT devices being made, and sold, globally. Some small shifts have been seen in large online platforms' age confirmation processes as a result of the AADC (Hern 2021), but what the effect on the device market will be remains to be seen. Yet, in situations where users are unaware of the risks of device use, either manufacturers have to make these risks clearer to the user, or mitigate those risks themselves — ideally both would happen, but in reality, there is typically little incentive for manufacturers to take such steps until such time as not doing so would incur penalties.

In a post-Brexit era, further policy — and potentially new legislation — may be discouraged by the current government: imposing higher standards of, for instance, cyber security controls (for instance ISO 27001) may form barriers to entry into the market. The UK government (at time of writing) had proposed the Data Protection and Digital Information Bill (2023), a significant break away from GDPR, in as much as the data subject, under the bill, would not be considered to have a fundamental right to data protection. This would have significant impacts upon the type of privacy that data subjects in the UK could hope for, at a time when devices have become increasingly opaque and take in more data than ever. **As the EU has already taken significant steps to impose ever stricter standards on technology firms (Digital Markets Act 2022), and continues to look to improve data subjects' use of data from home IoT devices (European Commission 2022), it is vital that the UK follows in their footsteps to avoid damaging its citizens' rights.** This could also take the form of **emulating EU calls for comprehensive labelling of consumer IoT products,** as described in the proposed (European Commission 2023).

One aspect of user protection that the UK has taken up alongside the EU is the right to repair for certain home electronic goods, including televisions and refrigerators (Harrabin 2021). **As these devices are expected to be repairable for up to ten years, so smart instances of these devices need to maintain appropriate software updates and usable security processes for this period.** This must happen to ensure that users are not put at risk for being careful with their devices, and that children do not need to learn that the ability to have devices on a budget does not come at the expense of its, and their, security.

Manufacturers also need to take strides to reduce the burden that

the heterogeneous nature of devices place on the consumer. This may seem like quite the departure from the discussion above, however the more recognisable the device interfaces and expected means of working (not to mention the ability for devices to talk to each other as standard), the more the cognitive burden will be reduced for users. Having the familiarity about what settings should look like to provide a secure setup should look like — or having terminology that is standard across all features — will go a long way to make users more secure, simply because they do not have to think about all the different possibilities of what right may look like for them.

8.2.4 Children need to be supported and involved more

A limitation of the feedback survey in Chapter 6 was that it only captured the voice of the parents; it did not ask those filling in the survey to report back on each family member, just on the family as a whole. Whilst that, obviously, included discussions, there were few direct reports of actions taken by the children; in one case, the family reported setting up extra parental controls, in practice further limiting the children's access to the Internet with less discussion. It is very likely that this example could be widely applied to device use in the home: children are spoken about, but not typically given much of an opportunity to get involved or exercise their own agency in the use of devices.

It was mentioned in Chapter 3.3.5 that UCD practitioners have long called for children to be involved as "protagonists" in design (Iversen, Smith and Dindler 2017). **This should be taken further: not only in considering how to make the core features of the devices better, but also in terms of the security features and exploring the unintended consequences that arise from standard application of device security settings.** We know that children do have views about the uses of their data (Dowthwaite et al. 2020), and can — and want to — participate in detailed discussions about data use and practice (Pothong and Livingstone 2022b). Given that manufacturers of devices that can be used by children should be giving thought to have evidence that their product(s) work "in the best interests of the child" (Information Commissioner's Office 2020b), this would be a very beneficial activity to undertake.

It is both understandable, yet also worrying, that children have such a limited window into household management of their devices. In many respects, this gap is not dissimilar to the involvement they have in the financial running of a house: children may gain experience of managing money through pocket money and small jobs, but are unlikely to have to take steps to pay significant household bills, or have access to understand the mechanisms of doing so, for example. Neither will they receive meaningful financial literacy training in school. This leaves a gap in which some children falter as they become adults — a 2021 survey found that 75% of 16-to-24-year-olds would turn to their parents over their place of education for advice on money (Student Beans 2021), and, despite financial education being on the secondary school curriculum since 2014, an interested charity noted how it was regularly not taught due to "a lack of resourcing, teacher training and prioritisation" (Staton 2022). Cyber security knowledge feels very similar: household management of devices, so much as it exists, is likely invisible to children: not taught at school, expecting to be taught by their parents — but this is extremely hard when, perhaps unlike money, the controls are hidden away, as they may be, in parents' smartphones. As explored in Chapter 4, this invisibility felt normal to parents with home IoT devices performing core household activities. It would, indeed, be ostensibly poor cyber security measure to allow children access to the controls, given the sharing of credentials that it may require. Yet, given industry calls for increased use of home IoT devices in new-build homes (techUK and GfK 2022) and the possible large-scale rollout of such devices in social housing in order for housing associations to meet obligations in relation to the upkeep of their housing stock (Levelling Up, Housing and Communities Committee 2022), reaching a point of joint understanding feels more important than ever.

Parents and children interviewed and surveyed in this research portrayed the learning provided by school as focusing only on the Internet as a place for socialising and commerce. **Curricula must be updated to capture not only the pervasive nature of the IoT, including exploring how the data collection from such devices is even more pervasive than that collected using the Internet, and also why the threats are different to the Internet accessed via a computer.** Helping children be able to better comprehend what and who may actually constitute a threat, and how to apply knowledge about cyber security skills to manage such threats, would be an excellent start.

However, enhancing school curricula is not enough to improve the cyber security knowledge within the home in the short term — not only do children not typically have the power in the familial relationship to engender change in their parents' activities, but accounts for the home IoT devices are unlikely to be theirs to manage. As Blum-Ross and Livingstone (2020) considered, the information exchange between school and parents is poor: there can be no expectation that parents would become significantly more knowledgeable simply because their children are learning more. Parents need to find means of educating themselves, and knowing how to extend this knowledge to their children, where the knowledge is not gained at school. **Further work should be undertaken by those third parties that hold themselves out as providing online safety advice for schools to provide to their children and parents.** Childnet, for instance, provides parents and carers with a Family Agreement template (Childnet 2021) — but only focusing on safe use of the Internet through a computer. Safer Internet Day, held in February each year, would be a perfect opportunity for organisations such as Childnet, the NSPCC[2] or UK Safer Internet Centre[3] (for example) and for schools to broaden the scope of their resources to include home IoT device safety — both for children, but also with resources for parents.

This leaves children in a difficult place — and their parents and guardians too. As explored in the findings, children are often given conflicting and confusing advice by their parents, which — just as their parents — means that they struggle to pick up strong cyber security measures. School education at present does not uniformly cover best practice enough to plug this gap. So this leaves children in a similarly tricky situation to the parents, in not understanding what to do. However, children — on the whole — may have the additional barrier of not being the owner or having access to make cyber security decisions about devices in the home. This leads to circumvention activities, as discussed in both the initial interviews and gameplay findings.

The complicated thing about circumvention is that, on the whole, children feel obliged to do it because the mechanism to keep them "safe" is too rigid. This came up repeatedly throughout all the pieces of research: cyber security measures do not work for families. They may work for individuals, without the need to

[2] `https://www.nspcc.org.uk/keeping-children-safe/online-safety/`

[3] `https://saferinternet.org.uk/`

interact with others — in this respect, for instance, password managers will work well in a corporate setting, where there is one primary device (the work machine) and one person using the password manager. But trying to extend solutions across device types or across groups of people with different needs becomes extremely hard to manage, and realistically brings us back to a fundamental issue: devices, on the whole, need one primary owner, who has to make the decisions. This creates the normalisation of security being handled by parents, which leads back to the issues discussed above: if there is no need to discuss cyber security because the decision is, by default, at the hands of the person associated with the device, then discussions will never happen.

A child-focused approach to cyber security awareness would encompass meaningful, up to date, ongoing education at school, enabling children to learn more about the technological environment in which they are growing up in, and in particular to foster a curiosity about the devices around them and how they work. This would, in part, provide children with the building blocks to start discussions. This could quite easily be brought into places of education through games, such as the one described here, allowing for enjoyment and play as a means of embedding knowledge. Whilst technical measures to solving the complex interplay between the primary users and others who are in the home do not exist — and may continue not to exist in meaningful ways for children — discussion based on up-to-date knowledge is arguably the only way for a family to understand what their goals and understandings about device use, and the surrounding security, are and should be.

8.3 Recommendations for stakeholders

The previous discussion section has provided several recommendations that arise from the findings of this work, in order that families can get to a place where they can use home IoT devices and have meaningful conversations relating to cyber security. These will now be presented below, in stakeholder groups. Some of the recommendations below relate specifically to UK legislation and government agencies, by virtue of the geographical location of the research. The remainder of the recommendations should obviously have a wider applicability. That being said, even where there are references to specific UK policies and school curricula, for example, it is likely that such recommendations could serve as a basis for similar considerations in other jurisdictions.

It is extremely important to notice that none of these recommendations fall upon families themselves. This research has shown that families are right at the start of their journeys around awareness of the need for more consideration of what cyber security measures would be appropriate to use when it comes to home IoT devices. Without change in the surrounding ecosystem, it is meaningless and unfair to put the burden of change upon families themselves.

8.3.1 Manufacturers, designers and developers

- **M1:** Do more to make the key threats of home IoT device use clearer at point of setup, and periodically throughout device use. *Relates to RFs 1, 2, 4, 5, 6, 7, 8, 9, 10, 19, 20, 21.*

- **M2:** Provide better guidance as to how to set up devices in a secure manner, based upon a number of commonly expected location and other use scenarios. *Relates to RFs 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 20, 21.*

- **M3:** Home IoT devices that are expected to be used by groups of people — especially children — should come with more stringent security measures set by default. *Relates to RFs 1, 2, 5, 8, 9, 10, 19, 20, 21.*

- **M4:** Consider how to use other authentication mechanisms than passwords: but, at a bare minimum, adhere to — and provide — password guidance from the governmental agencies in which devices are sold about best practice. *Relates to RFs 1, 7, 9, 10, 20, 21.*

- **M5:** Be upfront about how long a device will have updated secure software for, and how users should be able to use the device safely after that time, or if support has to be stopped sooner (in case of bankruptcy, for example). *Relates to RFs 2, 4, 7, 8, 21.*

- **M6:** Work to reduce the friction — and subsequent security risks that people may inadvertently create — caused by heterogeneity of devices. *Relates to RFs 1, 2, 4, 5, 6, 7, 21.*

- **M7:** Include children (or entire families) in UCD of security features to work toward measures that work for this user group. *Relates to RFs 1, 10, 11, 12, 15.*

8.3.2 Policymakers and governmental bodies

- **P1:** Update school curricula in all Key Stages to reflect the ubiquitous nature of the Internet and explicitly cover the practical application of cyber security across all device types that children may encounter in the home. Education must not focus only upon online safety. Schools specifically should look to find more creative means to discuss these issues to avoid boredom and repetition. *Relates to RFs 1, 2, 3, 7, 8, 10, 19, 20, 21*

- **P2:** Consider the wider use of awareness campaigns for core cyber security messages (such as "three random words"), as well as raising awareness of the role of the NCSC. Poster campaigns, short slogans and promotion of positive behaviour by government agencies and trusted members of society, whether in a personal capacity or through platforms, such as TV shows or recognised websites, may serve to normalise good cyber security measures. *Relates to RFs 2, 3, 5, 6, 7, 8, 9, 10, 19, 20, 21*

- **P3:** The PSTI Act must be reviewed and expanded as ongoing analysis recognises the need to avoid further harms arising from home IoT devices. *Relates to RFs 1, 2, 4, 8, 21*

- **P4:** The UK must look to keep in lockstep with the EU on core aspects of technology governance and legislation, including data protection regimes. *Relates to RFs 1, 2, 4, 8, 15, 21*

- **P5:** The UK government must consider ways of emulating certification schemes, whether voluntarily or mandatorily, such as that set out in the recently proposed amendment to the EU Cybersecurity Act (European Commission 2023). This will allow consumers to recognise, at point of sale, a device or manufacturer that can meet pre-defined security criteria. *Relates to RFs 1, 2, 4, 8, 21*

8.3.3 Academic community

- **A1:** Continue to research aspects of both specific technical and sociotechnical risks arising from home IoT devices, and ensure that such findings are disseminated in ways that can be understood by the public and effect change through policy and with manufacturers. *Relates to RFs 8, 9, 10, 23, 24, 15, 18, 19, 20, 21*

- **A2:** Continue to research the impact of the introduction of home IoT devices, and ubiquitous computing, as part of the normalisation of personal data use and the subsequent cyber security risks that this implies to both adults and children alike. *Relates to RFs 1, 2, 4, 8, 10, 15, 19, 20, 21*

8.3.4 Other stakeholders

- **O1:** ISPs must provide more guidance and support in setting up and maintaining a secure home network. *Relates to RFs 1, 2, 6, 7, 8, 9*

- **O2:** Internet safety organisations must broaden the remit of advice and resources given from online safety to include ubiquitous computing and harms arising from home IoT device use. Use these resources at key moments in the year (such as Safer Internet Day) to help schools, as mentioned in Recommendation P1, create engaging teaching methods and provide resources to share at home. *Relates to RFs 1, 2, 3, 4, 5, 6, 7, 9, 10, 14, 15, 19, 20, 21*

8.4 Limitations and future work

8.4.1 Limitations

As is the nature of all qualitative work, appendices and detailed methodology have been provided as a means of explaining how replication should be possible, although replication of process may yet end up with not only a different data set to analyse, but a different set of conclusions based upon that data set. Our findings can be said to be applicable to the situation that families — where families are strictly defined only as those with school-aged children living with them (in itself a limitation of the work) — found themselves in the UK, at the time of undertaking the research, and being able to participate in the research. Parenting methods, trust in government, governmental entities and consumer protections vary throughout the world: future work could be undertaken to understand where the findings of this piece of research may differ in other jurisdictions and regions globally. Taking the EU Kids Online survey as an example, which in its 2020 review, looked at online behaviours of children in 19 EU countries (Smahel et al. 2020), it may even be beneficial to scale such research up to look at the security differences in home IoT devices between countries: as devices are sold globally, so their use, and misuse, need to be understood globally too. Of course, basing research in the home in the period 2020-2022 may end up with results that may be less applicable in future years because of the initial, and ongoing changes required to life as a result of the COVID-19 pandemic.

As often happens in research relating to the home and family life, there was an over-representation of women participating in both the surveys and the interviews. Although this may serve to skew some responses, as women may have a tendency to underplay their technology knowledge (Rode 2010; Branley-Bell et al. 2022), this is to some degree balanced by the input of other family members in the interview process, and the aim of having entire families undertake the session in the game research. That said, in families where only one adult attended the sessions, with one exception (due to illness on the part of the wife), the adult was a woman, perhaps meaning that there is a slight blind-spot in the results as they did not include any obviously single-father families.

One aspect that arose during interactions with participants was the lack of a common understanding as to what a home IoT device was — and in particular, why some devices would be included, and others, like laptop computers, smartphones and tablets, would not be. This continues to be a difficult problem when trying to isolate particular aspects of usage and security. Arguably this problem is one that the PSTI Act has continued to conflate, given the equal applicability of the new act to those devices captured in the original DCMS Code (Department for Digital, Culture, Media and Sport 2018), as well as computers, smartphones and tablets.

There are limitations to using Prolific as a platform (and those platforms like it) for recruiting survey participants.[4] There is likely to be sampling bias in terms of the type of person who would consider being recruited to participant in surveys through such a platform. Recent research into the generalisability of questions of perceptions and knowledge around cyber security measures, with US respondents on Prolific, found that they were generally in line with external population polling in relation to perceptions around security, but had more knowledge than the average population (Tang, Birrell and Lerner 2022). Although based upon participants in the US, it is likely that this is the case in the UK too. However, even in the case that participants have provided answers that reflect a higher level of knowledge than the general population, the overall outcomes show a need for further support: if this is true of the relative experts on Prolific, it is only going to be more so in the general population. It must be considered also that the research is focusing on technology that is, at present, largely discretionary in nature; as such the higher proportion of employed participants may not be entirely surprising.

This research looked at the way in which families considered and, ultimately, made changes (or not) to the cyber security setup of their home IoT devices. It was intentionally not focused in a way that considered psychological or behavioural methods to facilitate changes, because of a lack of explicit researcher expertise in the area.

8.4.2 Future work

There are many directions in which future work in this field could progress. As mentioned in Section 8.4.1 above, these results are specific to the UK, during the period 2020-2022: replication of any or all of the individual pieces of research in different countries or in future years, when home IoT devices are more embedded in homes as a means of reducing energy consumption, for example, may yield different findings. Different cultures have different parenting styles, and it would be interesting to understand whether the ultimate finding of the importance of family discussion might be broadly applicable across the world. It may also be of vital importance to be more specific about the demographic groups covered: how would the findings differ in families with different structures and living situations

[4] For example, Amazon's MTurk `https://www.mturk.com/`.

than most of the families involved here? What would be the impact of multi-generational households, or situations where family members cannot freely, or safely, discuss issues of security together because of reasons of, *inter alia*, disability, family breakdown, or domestic abuse?

As mentioned above, because of the skills of the researcher, this work did not focus on behavioural or psychological interventions that could have been introduced. Future work could look more closely at the difficulties that power relationships, for example, might bring into managing cyber security between parents and children, particularly as children grow into teenagers. It would also be beneficial to consider whether families would be a particular target for the use of existing behavioural tools, such as nudges, in their cyber security setup.

In addition, other future work could look more at the specifics of threats to home IoT devices. This thesis considered threats and devices extremely generally: there would be benefit in exploring precisely which threats are relevant to which devices, and what the mitigating factors — whether technical in nature or more related to security behaviours could be. More work could also be carried out to understand how to design specific features to encourage appropriate cyber security behaviours of home IoT device users.

Due to the resources and time limitations of the final piece of research, it was not feasible to extend the final survey with gameplaying families beyond one week. It would have been valuable to extend out the final stages of the game research, as a week is a short period of time to measure changes made — and cannot necessarily say anything about the longer-term value of the knowledge gained from the game.

There is some possibly more concrete future work that can occur in relation to the game. During the course of this piece of research, children raised the idea of playing the game at school, and other participants asked why the game was not online, given the subject. Both of those permutations — a version that can be played at school, and an online version — could be created, based upon this work. Although the criteria for determining the success of the game as a way of learning about cyber security would have to be different, it could be extremely beneficial to have versions of the game that can be distributed amongst schools, and also more widely as an online version.

8.5 Concluding summary

This work has explored how UK families manage and discuss the cyber security of home IoT devices. In order to do this, four pieces of research were undertaken, and analysed through the framework of a version of the Transtheoretical Model of Behaviour Change (TTM) (as conceived by Faklaris, Dabbish and Hong (2018)).

Interviews and surveys with families (or family representatives) showed how little families seemed to know about, or consider cyber security in relation to home IoT devices at all, and in many cases seemed to consider cyber security to be one and the same as online safety. In terms of TTM, this showed that participant families exhibited signs of being at the precontemplation stage of adopting cyber security — that is to say, not even at a stage of knowing it would be necessary. Such a state would require awareness raising to move further through the cycle.

Subsequently, a review of information about cyber security for devices online found that it is almost impossible to get targeted, appropriate advice around home IoT device security online, thus hindering the ability to raise awareness. An autoethnographic diary study explored just how rarely cyber security does come up in conversation, even when the family is interested — and just how difficult it is to have those conversations when it does come up. This helped the researcher to understand more keenly why families may have such little awareness of the appropriate cyber security measures to use in relation to home IoT devices.

Finally, as a result of seeing the lack of awareness and available information on the subject in the prior pieces of research, the decision was taken to design a game with families to consider the final research question. This research would give the opportunity to see how well families would respond to being given information about appropriate cyber security measures. Framed in terms of TTM, this could allow participant families to move from a state of precontemplation further around the cycle, by providing the structure to raise awareness and also, perhaps, motivation to make a change. The reaction to the information used in the board game, too could also be used to see where other forms of intervention may be needed. The UCD aspect of this piece of research resulted in the creation of a board game that received high enjoyment and learning ratings from participants; it also showed that playing the game made it more likely for those families to alter elements of their cyber security setup than in the control group (who did not play the game). There were still many elements in which external interventions are required — recommendations for stakeholders have been listed out to help families in the future. There is the potential for future work, to see if the game could be adopted for use in schools, or made widely available as an online version.

Appendix A

Initial survey questions

A.1 Key to questions

Questions with a filled bullet point denote a single response question.
Questions with am empty bullet point denote that multiple choices are possible in an answer.
Every "other" option has a text box that must be populated if chosen.
The questions for Device 1 and 2 are the same, so will only be included here once.
If a survey participant signals that they only have 1 device, they will be taken to the section on "Support for digital technologies".
Italicised questions only pop up if the initial question is answered "yes" (or, in one case "no").
All questions are mandatory; in the case that an indented question appears, it becomes mandatory.

A.2 Household Information

How many adults (18+) live in your house? (choose one)

- 1
- 2
- 3
- 4

- 5
- 6+

What is/are the age ranges of child(ren) in your house? (choose all applicable)

- ○ 0-5
- ○ 6-10
- ○ 11-15
- ○ 16-17

A.3 Devices

What devices do you currently own or have in your household?

- ○ Connected children’s toys
- ○ Connected baby monitors
- ○ Connected smoke detector
- ○ Connected door lock
- ○ Connected doorbell
- ○ Other connected safety-relevant product
- ○ Smart camera
- ○ Smart TV
- ○ Device to connect smartphone to TV (e.g. Chromecast, Fire Stick)
- ○ Smart speaker
- ○ Connected home automation system
- ○ Connected alarm system
- ○ Connected thermostat
- ○ Connected heating or air conditioning unit
- ○ Connected fridge/freezer
- ○ Connected washing machine/tumble dryer

○ Other smart kitchen appliance

○ Smart home assistant

○ Smart lighting

○ Smart plugs

○ Smart kitchen appliance

○ Smart vacuum

○ Smart toothbrush

○ Smart scale

○ Other smart personal hygiene device

○ Smart printer

○ Smart meter

○ Other device type not listed

A.4 Specific Devices

[At this point, user selects device one and two, based upon the list above]

When was it bought?

- In the last 6 months
- In the last year
- In the last two years
- More than two years ago

What was the purpose of buying the device?

○ Make specific tasks easier for a certain family member (or members)

○ Make specific tasks easier for all family members

○ Device looked fun

○ To work alongside other devices

○ To optimise resource use (water, energy etc)

○ Landlord required it

○ Utility company/other service provider required it

○ It wasn't bought for the smart/connected features

Was there discussion about buying the device amongst the household members (including children) before it was bought?

- Yes
- No
- We did not make the decision to have the device in the house
- I don't remember

If yes, what did you discuss?

○ *Whether having the device would solve a particular problem*

○ *Who would use the device*

○ *If everyone (including children) liked the idea of having the device in the house*

○ *If everyone (including children) understood what the device did*

○ *If all adults liked the idea of having the device in the house*

○ *If all children liked the idea of having the device in the house*

○ *If all adults understood what the device did*

○ *If all children understood what the device did*

○ *Whether everyone would be able to use the device*

○ *If having the device would stop household members doing anything*

○ *Other*

Did the household member buying the device research it prior to buying it?

- Yes
- No
- I don't know

If yes, what was researched?

- ○ *Customer reviews on the Internet*
- ○ *Customer reviews from other sources (word of mouth)*
- ○ *Consumer body reviews (e.g. Which?)*
- ○ *Cost of device relative to other products*
- ○ *What the device looked like*
- ○ *Whether the device was compatible with other devices or technology in the house*
- ○ *Reputation of the manufacturer*
- ○ *Security features*
- ○ *Privacy features*
- ○ *How many users could use the device*
- ○ *Data retention/privacy policies*
- ○ *What associated apps looked like/how well they worked*
- ○ *Other*

When the device was set up, were there detailed instructions?

- Yes
- No
- I don't remember

If yes, were these instructions:

- *Physically printed and within the packaging*
- *On a website that was signposted to during setup of the device*
- *Other*

Did the household member setting up the device read the instructions?

- *Yes*
- *No*

- *I don't know*

Does the device rely on an app?

- Yes
- No
- I don't know

Did setup involve changing the device's password?

- Yes
- No
- I don't know

Did setup require individual users' details to be input?

- Yes
- No
- I don't know

Did setup require individual user accounts to be created?

- Yes
- No
- I don't know

If yes, do you know how the user accounts are created and maintained?

- *The user who set it up originally has more control than other users*
- *A user other than the one who set it up originally has more control than other users*
- *Each user can decide for themselves once their account is set up*
- *Predefined account restrictions based upon, for example, age*
- *Other*

If users have different types of access to the device, do you know what this is based upon?

○ *Having their own access to the app that controls the device*

○ *Based upon the settings that the account was set up with*

○ *Age restrictions*

○ *Other*

Do you know how you would completely delete the information the device has collected?

- Yes
- No
- I don't know

If yes, how?

○ *Send an email to the manufacturer*

○ *Can be done through the device or associated app*

○ *Can be done through logging in to the manufacturer's website*

○ *Other*

Has your current device ever broken? (or a similar device carrying out the same activity)

- Yes
- No
- I don't remember

If yes, did you

○ *Find a way to repair the device*

○ *Directly replace it, carrying over account information*

○ *Directly replace it, without carrying over account information*

○ *Replaced it with a different model/brand*

○ *Other*

Do you know how the device was broken?

○ *Broken by adult household member*

○ *Broken by child household member*

○ *Broken by other person (or pet)*

○ *Battery stopped working*

○ *Functionality stopped working*

○ *Stopped working after a software update*

○ *Other*

Who was most impacted by the breaking of the device?

- *Me*
- *Other adults in the house*
- *Child(ren)*
- *Landlord/service provider*
- *All of us*
- *We were not that bothered*
- *Other*

If the device broke tomorrow, what would be your major concerns?

○ How it should be replaced

○ The data that might have been lost

○ The functionality that has been lost

○ Inability to use paired/compatible devices

○ It is not my device; needs to be replaced by/for someone else (such as a landlord, utility company)

○ Other

Do you know how long for, or until when, the software on the device is supported until?

- Yes

- No
- I don’t know

Does one person in the house take ownership of managing the device?

- Yes; me
- Yes; another adult
- Yes; a child
- No one person in the household
- Managed by a landlord

Was this a deliberate decision by the household?

- Yes
- No
- I don’t know

Have there ever been any problems arising from this decision?

- Yes
- No
- I don’t know

If yes, and managed by no one person: what were they?

○ *Forgotten password/login credentials*

○ *Disagreement over the best ways to manage the device*

○ *Disagreement about user permissions*

○ *Other*

If managed by one person: what were they?

○ *User with control forgot password/login credentials*

○ *User with control not present when needed*

○ *User with control had to change phone or other means of managing device*

○ *User with control does not always understand what other users need from the device*

○ *Other*

Does everyone in the household use the device in the same way?

- Yes
- No
- I don't know

If no, what sort of things do different household members do differently?

○ *Use different device settings*

○ *Interact with it in different ways (through app, or voice)*

○ *Use different features*

○ *Not use the device at all*

○ *Other*

Do you have to help the child(ren) in the house to use the device?

- Yes; just me of all the adults in the house
- All/most of the adults in the house do
- Another adult in the household does; not me
- No
- Other

If yes, What do you (or other adult(s) in the household) have to do for them?

○ *Let them use a smartphone to control the device through an app (or equivalent)*

○ *Speak/interact with the device for them*

○ *Explain how to interact with the device*

○ *Explain what the device can and cannot do*

- ○ *Stop the child(ren) from using the device in a way that might physically damage it*
- ○ *Stop the child(ren) from using the device in a way that might damage the service it provides*
- ○ *Let them use a smartphone or device to access the data the device has collected*
- ○ *Other*

Do you feel you, or the other adult(s) in the household, have to control your child(ren)'s interactions with the device?

- ● *Yes*
- ● *No*
- ● *I don't know*

How do you (or the other adult(s) in the household) do this?

- ○ *Use the device with them*
- ○ *Use the device for them*
- ○ *Explaining how to use the device*
- ○ *Restricting their use of the device*
- ○ *Explaining how the device works*
- ○ *Other*

What are your concerns with having to control your child(ren)'s use of the device?

- ○ *I don't know much about how the device works*
- ○ *I didn't get much information about how to setup the device properly*
- ○ *It takes up too much of my time*
- ○ *They seem to know how to use the device better than me*
- ○ *They rely on another adult than me*
- ○ *They get different advice from different adults in the house*

○ *I don't have any concerns*

○ *Other*

Do you do help with or control the use of devices differently for the different children within your house?

- *Yes*
- *No*
- *We only have one child in the house*

What is this based on?

○ *Child's age*

○ *Child's skill with the device*

○ *Child's level of interest in the device*

Do you know if the child(ren) use the device by themselves?

- Yes
- No
- I don't know

Do they find it harder to use the device than the adults in the household do?

- *Yes*
- *No*
- *I don't know*

If yes, why do they find it harder?

○ *Interaction with the device is harder*

○ *They need an app (that they don't have access to) to make the device work*

○ *They need an app (that they cannot properly use) to make the device work*

○ *They don't understand the limitations of the device*

○ *They cannot use the device interfaces properly*

○ *Other*

Do they find it harder to use the device than any equivalent non-smart device that you have had in the past? (for example, do they find it harder to use a Smart TV than a TV with a DVD player?)

- *Yes*
- *No*
- *I don't know*

Do you have concerns with your child(ren) using the device?

○ Physically breaking the device

○ Having to use an app to manage the device

○ Deleting data or settings from the device

○ Finding out information about your or another adult in the household's use of the device

○ That they may change the settings

○ That the device is not meant for their use (e.g. a smart meter)

○ That their using the device takes up too much of your time

A.5 Support for Digital Technology Use

Who or where do you turn to for support with digital technology issues?

○ Other adults in my household

○ Child(ren) in my household

○ I don't need support

○ Friend(s)

○ Family outside of the household

○ The Internet

○ Paid support

○ Other

Have you ever been a victim of a cybercrime or data breach?

- Yes
- No
- I don't know

If yes, did you incur a loss as a result of this?

- *Yes*
- *No*
- *I don't know*

Are you aware of the manufacturers of any of the devices you own publicly reporting a security breach?

- Yes
- No
- I don't know

A.6 Children's Education and Digital Technologies

Do you know if your child(ren)'s school syllabus has covered the following topics?

○ Harmful online content

○ Stranger danger

○ Use of strong, unique passwords

○ Personally identifiable data

○ Cyber crime

○ Cyber bullying

○ Malware (including viruses, or ransomware)

Have you ever discussed any of the following topics with your child(ren)?

○ Screen time

○ Talking to strangers online

○ Using strong and unique passwords

○ How to minimise risks of becoming a victim of malware

○ How digital technologies might use personal data

○ What it means for a device to be "smart"

○ How a device uses personal data to become "smart"

○ The importance of software updates

○ What data might identify or reveal about you

Appendix B

Initial interview questions

B.1 *

Device questions

To each adult (+16) household member individually:

- How do you use the device?
- Do you have a separate account to other house members?
- Have you ever tried to change the settings of the device? If so, can you tell me more about that?
- What information do you think the device has about you?
  - How do you feel about that?
  - Who do you think can access that information?
- Do you think the device is useful?
- Do you use the device for the purpose that you bought it?
- What would you change about the device?
- Do you have to use workarounds to use the device in the way you want to?
- Does the device work as well for every member of the household?

- Do you intend on buying or having any more devices installed in your home in the next year?
- If so, which and why?

To each primary school aged child (4-11):

- How do you use the device?
- Do your parents have to help you?
- Do you have your own account? If so, does that limit what you can do with it? Do your parents control what you can do (e.g. with an app)?
- Do you do different things with the device to the adults in the house or your siblings?
- Can you tell me how you think the device works?
- What do you like about the device?
- What would you change about the device?
- Do you know how to turn the device on or off, or make changes to how it works? Have you tried to do this?

To each 12-16 year old child:

- How do you use the device?
- Do you have a separate account to other house members? Do your parents have to monitor what you do with the account?
- How do you think the device works?
- What information do you think the device has about you?
  - How do you feel about that?
  - Who do you think can access that information?
- Do you think you use it differently to your parents and siblings?

- Have you ever tried to change the settings of the device? If so, can you tell me more about that?
- Do you think the device is useful?
- What would you change about the device?
- Does the device stop you from doing things, physically or virtually?

B.2 *

Cyber security knowledge

Questions to adults:

- How well do you think you have secured the devices you have in your home?
  - Can you give details?
  - Is there one person in the house that is more likely to manage issues with technology?
    - Is this because of necessity or choice?
    - Do the other members of the household wish they could do more?
- What do you consider to be the biggest risk that you have with the IoT devices in your home?
  - Is there anything you feel you could do immediately to minimise that risk?
  - What else would you like to see done to minimise that risk? By whom?
- Are you aware of ever having been the victim of a cyber crime or data breach?
- Who manages the cyber security aspects of the devices that you use in the home?
  - Is that an intentional choice?

- Which sources to do you use to get cyber security information?
  - Are you aware of educational schemes run by the government or other non-governmental organisations? If so, have you used them, and did they help?
- What would be your ideal method of becoming informed about cyber security issues that might affect you?
- Are you aware of any issues (on the news or otherwise) that have been raised about the security of IoT devices?
  - How does that make you feel?

Questions to all children:

- What have you learned at school about computers and the Internet?
  - Can you describe to me what you know about staying safe when using the Internet?
  - Do you talk about what you've learned with your family?

Questions to 12+ children:

- How much knowledge do you think you have about using the Internet compared to your parents?
  - Have you ever given them help?
- Could you describe to me what you think the biggest risks of using Internet-connected devices in the house are?
  - What changes would you like to make to stop those risks happening?

Appendix C

Initial interviews code book

Codes/subcodes	Description of subcode heading
Use of devices within the home	
Family relationship with devices	Elements of the family's relationship with home IoT devices
Limitation of use	
Lack of trust	
Negative managing experiences	
Positive/neutral managing experiences	
Controls that people have	
Negative device experiences	
Positive device experiences	
Joint device use	
Adult relationship with devices	Specific instances of how adults use home IoT devices, as described by both adults and children
Adult device use	
Child relationship with devices	Specific instances of how children use home IoT devices, as described by both adults and children
Overly comfortable with devices	
Child device use	
Child ease of use	
Child managing or altering device	
Child circumvents restrictions	

Continued on next page

Codes/subcodes	Description of subcode heading
Child is not careful with devices	
Child is careful with devices	
Confusion over device knowledge	Examples of where any interview participant expressed a lack of knowledge about their home IoT devices
Don’t understand how device works	
Lack of personal confidence	
Incompatibility	
How do devices work	Topics that came up when any interview participant explained their understanding of how home IoT devices worked
Data devices have	
Always listening?	
Never considered	
Not sure how secure it is	
Comfortable about use in home	
Not comfortable about use in home	
How much can they do with the data?	
Download of personal data	
About the devices	Explanations of how interview participants viewed the devices and why they bought them
Just like any other white good	
Why bought?	

Continued on next page

Codes/subcodes	Description of subcode heading
Parental relationship with devices	How parents view home IoT devices with respect to their children's use
Devices aren't different to other technologies	
Content concerns	
Destruction of device	
Kid's filter is too restrictive	
Concerns for children	
Educating yourself to look after children	
Where to get support from	Where participants explained they would get information about security, should they need it
TV programmes	
Online — specific source	
YouTube	
Bank	
Government	
No idea	
Police	
Family	
Friends	
Online — generic	

Continued on next page

Codes/subcodes	Description of subcode heading
Concerns	All concerns listed, by any participant, about digital technology use
Privacy	
Security	
Unintended consequences	
Parental tracking	
Lack of parental control	
Restrictions	
Children believing everything online	
Child/restricted accounts	
Risks	The risks that participants saw in relation to using home IoT devices
Data breach	
Time waste	
Physical damage	
Malfunction	
Inappropriate content	
Viruses	
Lack of accountability for online info	
Identity Theft (real or accidental)	
Unsolicited contact from strangers	

Continued on next page

Codes/subcodes	Description of subcode heading
Scams/financial fraud	
”Hacking”	
Doxxing/identifying yourself	
Information theft	
Parent/child discussion	Types of family discussions described by participants
Discussing things learned at school	
Discussion as a means of solving problem	
Children learn from parents	
Safeguarding	
Child telling parent what to do	
Cyber security management in the home	
Knowledge	Instances in which the participant’s level of, or means of acquiring, knowledge were explained
Tech negatively in the news	
Tech in the news	
How to do it	
Not that concerned	
Self-confidence	
Too difficult to think about	
Good level of security in the house	
Unsure of level of security in the house	

Continued on next page

Codes/subcodes	**Description of subcode heading**
What is taught at school	
What school could cover	
Strategies	Examples of specific cyber security strategies
Turning off Wi-Fi	
Password manager	
Awareness of malicious things online	
Smishing	
Old devices	
Biometrics	
2FA	
Data deletion	
Antivirus	
Password reuse/weak passwords	
Personal data use	
Passwords	
Software updates	

Appendix D

Word frequency analysis background documentation

This appendix details out the 50 papers used for the word frequency analysis undertaken in as part of the Cyber Security Awareness Information Review, and the top 100 results generated from that analysis.

Papers used for word frequency analysis

Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight*, *20*(2), 150–161. https://doi.org/10.1108/FS-08-2017-0043

Ahmad, N., Mokhtar, U. A., Fauzi, W. F. P., Othman, Z. A., Yeop, Y. H., & Abdullah, S. N. H. S. (2018). Cyber Security Situational Awareness among Parents. *2018 Cyber Resilience Conference (CRC)*, 1–3.

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62–68.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2017). Enhancing cyber security awareness with mobile games. *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, 129–134.

Arora, B. (2019). Teaching cyber security to non-tech students. *Politics*, *39*(2), 252–265. https://doi.org/10.1177/0263395718760960

Ban, Y., Okamura, K., & Kaneko, K. (2017). Effectiveness of Experiential Learning for Keeping Knowledge Retention in IoT Security Education. *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 699–704. https://doi.org/10.1109/IIAI-AAI.2017.206

Bidmeshki, M., Reddy, G. R., Zhou, L., Rajendran, J., & Makris, Y. (2016). Hardware-based attacks to compromise the cryptographic security of an election system. *2016 IEEE 34th International Conference on Computer Design (ICCD)*, 153–156.

Bresch, C., Hély, D., Papadimitriou, A., Michelet-Gignoux, A., Amato, L., & Meyer, T. (2018). Stack Redundancy to Thwart Return Oriented Programming in Embedded Systems. *IEEE Embedded Systems Letters*, *10*(3), 87–90.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining Technology Threat Avoidance Theory. *Communications of the Association for Information Systems*, 380–407. https://doi.org/10.17705/1CAIS.04422

Chatterjee, U., Santikellur, P., Sadhukhan, R., Govindan, V., Mukhopadhyay, D., & Chakraborty, R. S. (2019). United We Stand: A Threshold Signature Scheme for Identifying Outliers in PLCs. *Proceedings of the 56th Annual Design Automation Conference 2019*, 1–2. https://doi.org/10.1145/3316781.3322480

Chattopadhyay, A., Christian, D., Ulman, A., & Petty, S. (2018). Towards A Novel Visual Privacy Themed Educational Tool for Cybersecurity Awareness and K-12 Outreach. *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, 159–159. https://doi.org/10.1145/3241815.3241883

Choong, Y.-Y., Theofanos, M. F., Renaud, K., & Prior, S. (2019). “Passwords protect my stuff”—A study of children’s password practices. *Journal of Cybersecurity*, *5*(1), tyz015. https://doi.org/10.1093/cybsec/tyz015

Chou, T.-S., & Jones, J. (2018). Developing and Evaluating an Experimental Learning Environment for Cyber Security Education. *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, 92–97. https://doi.org/10.1145/3241815.3241855

Eustace, K., Islam, R., Tsang, P., & Fellows, G. (2018). Human Factors, Self-awareness and Intervention Approaches in Cyber Security When Using Mobile Devices and Social Networks. In X. Lin, A. Ghorbani, K. Ren, S. Zhu, & A. Zhang (Eds.), *Security and Privacy in Communication Networks* (Vol. 239, pp. 166–181). Springer International Publishing. https://doi.org/10.1007/978-3-319-78816-6_13

Filipczuk, D., Mason, C., & Snow, S. (2019). Using a Game to Explore Notions of Responsibility for Cyber Security in Organisations. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3290607.3312846

Garae, J., Ko, R. K. L., Kho, J., Suwadi, S., Will, M. A., & Apperley, M. (2017). Visualizing the New Zealand Cyber Security Challenge for Attack Behaviors. *2017 IEEE Trustcom/BigDataSE/ICESS*, 1123–1130.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Hadlington, L. (2018). *Employees Attitude Towards Cyber Security And Risky Online Behaviours: An*

Empirical Assessment In The United Kingdom. https://doi.org/10.5281/ZENODO.1467909

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, *95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

Holdsworth, J., & Apeh, E. (2017). An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector. *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*, 111–117.

Jixing, L., Yu, W., & Bin, Q. (2018). Discussion on Cyber Security Awareness and Awareness Model Building Based on Connectionism. *2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC)*, 259–263.

Katsantonis, M., Fouliras, P., & Mavridis, I. (2017). Conceptual analysis of cyber security education based on live competitions. *2017 IEEE Global Engineering Education Conference (EDUCON)*, 771–779.

Katsantonis, N. M., Kotini, I., Fouliras, P., & Mavridis, I. (2019). Conceptual Framework for Developing Cyber Security Serious Games. *2019 IEEE Global Engineering Education Conference (EDUCON)*, 872–881.

Kim, B.-H., Kim, K.-C., Hong, S.-E., & Oh, S.-Y. (2017). Development of cyber information security education and training system. *Multimedia Tools and Applications*, *76*(4), 6051–6064. https://doi.org/10.1007/s11042-016-3495-y

Knox, B. J., Lugo, R. G., Helkala, K., & Sütterlin, S. (2019). Slow Education and Cognitive Agility: Improving Military Cyber Cadet Cognitive Performance for Better Governance of Cyberpower. *International Journal of Cyber Warfare and Terrorism*, *9*(1), 48–66. https://doi.org/10.4018/IJCWT.2019010104

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, *8*, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867

Lehto, M. (2016). Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences: *International Journal of Cyber Warfare and Terrorism*, *6*(2), 15–31. https://doi.org/10.4018/IJCWT.2016040102

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). *Cyber Security Awareness and Its Impact on Employee's Behavior*. *268*, 103–111. https://doi.org/10.1007/978-3-319-49944-4_8

Lodgher, A., Yang, J., & Bulut, U. (2018). An Innovative Modular Approach of Teaching Cyber Security across Computing Curricula. *2018 IEEE Frontiers in Education Conference (FIE)*, 1–5.

Martin, F., Wang, C., Petty, T., Wang, W., & Wilkins, P. (2018). Middle School Students' Social Media Use. *Journal of Educational Technology & Society*, *21*(1), 213–224.

Mathoosoothenen, V. N., Sundaram, J. S., Palanichamy, R. A., & Brohi, S. N. (2017). An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform. *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence - CSAI 2017*, 199–202. https://doi.org/10.1145/3168390.3168397

Micallef, N., & Arachchilage, N. A. G. (2018). Security questions education: Exploring gamified features and functionalities. *Information & Computer Security*, *26*(3), 365–378. https://doi.org/10.1108/ICS-03-2018-0033

Moallem, A. (2019). Cyber Security Awareness Among College Students. In T. Z. Ahram & D. Nicholson (Eds.), *Advances in Human Factors in Cybersecurity* (Vol. 782, pp. 79–87). Springer International Publishing. https://doi.org/10.1007/978-3-319-94782-2_8

Orozova, D., Kaloyanova, K., & Todorova, M. (2019). *Introducing Information Security Concepts and Standards in Higher Education*. https://doi.org/10.18421/TEM83-46

Pham, H. C., Brennan, L., Parker, L., Phan-Le, N. T., Ulhaq, I., Nkhoma, M. Z., & Nhat Nguyen, M. (2019). Enhancing cyber security behavior: An internal social marketing approach. *Information & Computer Security*, *28*(2), 133–159. https://doi.org/10.1108/ICS-01-2019-0023

Rajamäki, J. (2018). Industry-university collaboration on IoT cyber security education: Academic course: 'Resilience of Internet of Things and cyber-physical systems'. *2018 IEEE Global Engineering Education Conference (EDUCON)*, 1969–1977.

Raval, R., Maskus, A., Saltmiras, B., Dunn, M., Hawrylak, P. J., & Hale, J. (2018). Competitive Learning Environment for Cyber-Physical System Security Experimentation. *1st International Conference on Data Intelligence and Security, ICDIS 2018, South Padre Island, TX, USA, April 8-10, 2018*, 211–218. https://doi.org/10.1109/ICDIS.2018.00042

Reid, R., & Van Niekerk, J. (2016). Decoding audience interpretations of awareness campaign messages. *Information and Computer Security*, *24*(2), 177–193. https://doi.org/10.1108/ICS-01-2016-0003

Roy, D. B., Alam, M., Bhattacharya, S., Govindan, V., Regazzoni, F., Chakraborty, R. S., & Mukhopadhyay, D. (2018). Customized Instructions for Protection Against Memory Integrity Attacks. *IEEE Embedded Systems Letters*, *10*(3), 91–94.

Samuels, A., Li, F., & Justice, C. (2017). Applying rating systems to challenge based cybersecurity education. *2017 International Conference on Computing, Networking and Communications (ICNC)*, 819–824.

Shabe, T., Kritzinger, E., & Loock, M. (2017). Scorecard Approach for Cyber-Security Awareness. In T.-C. Huang, R. Lau, Y.-M. Huang, M. Spaniol, & C.-H. Yuen (Eds.), *Emerging Technologies for Education* (Vol. 10676, pp. 144–153). Springer International Publishing. https://doi.org/10.1007/978-3-319-71084-6_16

Shinde, P. S., & Ardhapurkar, S. B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, 1–5.

Tirumala, S. S., Valluri, M. R., & Babu, G. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 1–6.

Trim, P. R. J., & Lee, Y.-I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224–238. https://doi.org/10.1016/j.indmarman.2019.04.003

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as “the three R’s”. *Heliyon*, *5*(12), e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

Wang, Y., Qi, B., Zou, H., & Li, J. (2018). Framework of Raising Cyber Security Awareness. *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, 865–869.

Wibowo, S. (2018). Enriching Digital Government Readiness Indicators of RKCI Assessment with Advance Https Assessment Method to Promote Cyber Security Awareness Among Smart Cities in Indonesia. *2018 International Conference on ICT for Smart Society (ICISS)*, 1–4.

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, *88*, 101636. https://doi.org/10.1016/j.cose.2019.101636

Zhang, J., Yuan, X., Xu, J., & Jones, E. J. (2019). Developing and Assessing Educational Games to Enhance Cyber Security Learning in Computer Science. *Proceedings of the ACM Conference on Global Computing Education*, 241–241. https://doi.org/10.1145/3300115.3312511

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 1–16. https://doi.org/10.1080/08874417.2020.1712269

Word Frequency Analysis – top 100 results

Word	Length	Count	Weighted Percentage (%)
security	8	4179	1.99
cyber	5	2648	1.26
information	11	1280	0.61
awareness	9	1090	0.52
students	8	699	0.33
social	6	659	0.31
knowledge	9	658	0.31
research	8	654	0.31
learning	8	632	0.30
education	9	631	0.30
based	5	574	0.27
system	6	530	0.25
computer	8	487	0.23
study	5	487	0.23
systems	7	483	0.23
behavior	8	474	0.23
training	8	463	0.22
using	5	462	0.22
attacks	7	451	0.21
university	10	443	0.21
users	5	434	0.21
attack	6	427	0.20
technology	10	418	0.20
network	7	409	0.19
level	5	387	0.18
internet	8	380	0.18
cybersecurity	13	373	0.18
analysis	8	364	0.17
management	10	359	0.17
participants	12	351	0.17
results	7	347	0.17
model	5	342	0.16
different	9	336	0.16
threat	6	336	0.16
threats	7	326	0.16
https	5	318	0.15
environment	11	307	0.15
people	6	307	0.15
engineering	11	302	0.14

international	13	291	0.14
password	8	291	0.14
online	6	290	0.14
media	5	288	0.14
table	5	281	0.13
journal	7	278	0.13
related	7	271	0.13
paper	5	267	0.13
passwords	9	266	0.13
survey	6	266	0.13
design	6	263	0.13
section	7	263	0.13
application	11	262	0.12
conference	10	262	0.12
software	8	261	0.12
individual	10	250	0.12
questions	9	249	0.12
however	7	247	0.12
human	5	245	0.12
tools	5	245	0.12
games	5	244	0.12
access	6	240	0.11
approach	8	237	0.11
process	7	229	0.11
found	5	226	0.11
challenges	10	222	0.11
group	5	219	0.10
school	6	218	0.10
employees	9	217	0.10
privacy	7	216	0.10
control	7	215	0.10
development	11	215	0.10
factors	7	212	0.10
marketing	9	210	0.10
number	6	209	0.10
behaviors	9	207	0.10
educational	11	206	0.10
issues	6	206	0.10
critical	8	202	0.10
provide	7	202	0.10
example	7	201	0.10
framework	9	201	0.10
protection	10	195	0.09

future	6	193	0.09
available	9	192	0.09
theory	6	191	0.09
communication	13	190	0.09
figure	6	188	0.09
making	6	188	0.09
reported	8	188	0.09
personal	8	187	0.09
staff	5	185	0.09
scenario	8	184	0.09
skills	6	184	0.09
various	7	183	0.09
within	6	183	0.09
methods	7	180	0.09
science	7	180	0.09
order	5	179	0.09
support	7	176	0.08
digital	7	175	0.08

Appendix E

Cyber security awareness review: Full list of advice and threats provided and the organisation types that provided them

E.1 Full number of instances of advice types given

Table 30: Full number of instances of advice types given

Advice type give	Number of instances
Strong passwords	149
Limit data access	145
Improve home networking	143
Disable devices	117
Automatic software updates	113
Use 2FA/MFA	61
Use VPN	50
Be cautious	49
Use anti-virus	48
Restrict children’s device use	45
Delete data	28
Don’t click links	29
Don’t use public connections/charging	28
Restrict physical location of device	25
Don’t use risky devices	24
Encrypt	23
Avoid 3rd party devices	22
Read privacy policy	22
Talk about use with all users	19
Use password manager	17
Wipe devices at the end of use	17
Back up data	16
Set up correctly	16
Know how devices work	15
Do not jailbreak/root	13
Log activity on devices	13
Understand data collection process	11
Have financial awareness	10
Research before you buy	8

Table 30 continued from previous page

Advice type give	Number of instances
Understand when end of life is	8
Use https (secure transmission)	6
Turn off when not in use	5
Use biometrics	5
Contact professionals for support	4
Don't use illegal materials	4
Enforce least privilege	4
Isolate infected devices	3
Replace devices at end of life	3
Don't use unnecessary devices	2
Investigate issues	2
Receive notifications	2
Reclaim accounts when lost	2
Segregate data	2
Use ad-blocker	2
Use credit card online	2
Use email to log data flows	2
Control Internet access	1
Don't use insecure connections	1
Regulation needed	1
Report crime	1
Use physical deterrent	1
Use TOR	1
Use virtual machine	1
Write down IMEI	1

E.2 Full number of instances of threat types given

Table 31: Full number of instances of threat types given

Type of threat	Number of instances
Unauthorised access	144
None specifically	37
Malware	22
Data theft	13
Botnet	9
Ransomware	8
Insecure devices	7
Phishing	7
Physical harm	6
Cyber attack	5
Loss or theft	5
Attack on availability	4
Burglary	4
Data loss	4
Financial fraud	4
Identity theft	4
Inappropriate content	4
Privacy breach	4
Spying	4
Accidental purchase	3
Children's lack of knowledge	3
Cyber bullying	3
Cyber crime	3
Data misuse	3
Fraud	3
Tracking	3
Corporate espionage	2
Credential theft	2
Eavesdropping	2

Table 31 continued from previous page

Type of threat	Number of instances
Lack of knowledge	2
Social engineering	2
APTs	1
Attack on confidentiality	3
Attack on integrity	1
Blastware	1
Complexity of system	1
Cyber predators	1
Cyber terrorism	1
Damage	1
Data collection	1
Devices acting unexpectedly	1
Domestic abuse	1
Encryption	1
Ghostware	1
Hacktivism	1
Hardware issues	1
Insecure wifi	1
Internet dependency	1
Relay attack	1
Romance scams	1
Scams	1
SQL injection	1
Stranger danger	1
Theft	1
Threats	1
Too much device use	1
Vandalism	1

E.3 Full number of instances of organisations

Table 32: Full number of instances of organisations

Type of organisation	Number of instances
Blog	79
Media	46
Industry	31
Cyber security firm	21
Forum	13
Anti-malware provider	9
Government	9
Not for profit/charity	5
Comparison site	4
Consumer Protection	3
Education	2
Research	3
Financial	2
Mobile phone distributor	1
Retailer	1
Security provider	3
Supra-national body	1
Reference	1

Appendix F

Autoethnographic diary study: daily diary prompts

Daily diary prompts

Prompt questions: home IoT device use and cyber security discussions
How did it arise?
Was the conversation home IoT device use or cyber security related?
How long did it last?
Did everyone participate?
Did the children engage (ask questions, seem to take it in)?
What questions did they ask?
Did they use metaphors/examples? What were they, and how did they seem to relate to the topic being discussed?
Have you discussed this before?
Did you ask any questions?
Did you use metaphors/examples from other areas? What were they?
Did this help in furthering the conversation or making a more meaningful interaction?
Did you refer to anything else?
Was it a helpful conversation? What went well? What didn't?
Were there any conversations on digital technologies or cyber security that you avoided having today? — About what? Why?

Appendix G

Autoethnographic diary study: code book

Autoethnographic diary study: codebook

Top-level code	**Sub codes**
Formal messaging around home IoT devices	
	Social media messages
	Formal education
Home IoT devices uses	
	Technology for connection
	Technology as means to an end
	Gatekeeping technology
	Technology with wrong features
	Technology as additional family work
Emotions generated by home IoT devices	
	Privacy Concerns
	Expensive tech
	Parental concern
	Not understanding what technology is trying to tell us
	Useful technology
	Attractive technology
	Frustrating technology
	Lack of knowledge
	Lack of agency
	Not having the words
	Uncertain risks
	Lack of interest
	Too much effort
Informal educational effort around home IoT devices	
	Technology and the outside world
	Cyber security talk with family
	Technology discussion with family

Appendix H

Initial game cards

This appendix provides the versions of the cards that were created for the initial version of the game.

Inside Threat Card

Threat: Someone in the house has tried to use your smartphone.

If you have the following cyber security card, you don't need to take further action:

Access codes for device apps

Your device cannot be used by people who don't have the access code.

If you don't have the card, roll the dice:

Odd Number: Your device settings have been changed. Skip a turn as you sort it out.

Even Number: They just wanted to look at some cat photos on your camera roll – no real harm for now...

Threat: Someone in the house has tried to buy something through your device.

If you have the following cyber security card, you don't need to take further action:

Turn off automatic purchases on your device.

Nothing can be purchased unless you approve it.

If you don't have the card, roll the dice:

Odd Number: Thankfully, nothing seems to have happened.

Even Number: Your device has been used to buy a £30 product. Pay £30.

Threat: A relative visits your home, and when looking at your device, presses some buttons, and some settings get deleted.

If you have the following cyber security card:

Profiles for devices

Skip a turn to restore everyone's profile, or pay £10 to get someone else to do it for you.

Threat: One of the children in the house has accessed content you're not happy with on your device.

If you have the following cyber security card:

Family discussion: device use

You have a short discussion based on what you've agreed before.

If you don't have the card:

Skip a turn to discuss ground rules with everyone else.

Threat: Someone has decided to play a joke on you by modifying the settings on your device.

If you have the following cyber security card, you don't need to take further action:

Use an authenticator app with your devices

Without having access to the authenticator app, they cannot log into the device.

If you don't have the card, roll the dice:

Odd Number: Nothing serious: they just wanted it to tell you a joke next time you started it.

Even Number: They've modified the settings and you can't make it turn on! Skip a turn as you perform a factory reset, or pay £10 to get someone else to do it for you.

Threat: You have a serious falling out with a neighbour who has, in the past, connected to your home wifi with their laptop and phone.

If you have the following cyber security card, you don't need to take further action:

Review devices on your network

You can make sure the neighbour's devices are not connected to your network.

If you don't have the card:

Skip a turn as you try to figure out if your neighbour has access, or pay £10 to get someone else to do it for you.

Threat: A friend of the youngest member of the family takes too much of an interest in your device. They are too young to understand how to use the device properly and accidentally delete some data.

If you have the following cyber security card, you don't need to take further action:

Back up devices

You have a copy of your data that you can restore.

If you don't have the card, roll the dice:

Odd Number: Thankfully, they've not deleted anything important.

Even Number: Skip a turn as you figure out what data's been lost, or pay £10 to get someone else to do it for you.

Threat: You need to do a project at home, that requires talking to lots of people over videochat about quite sensitive things you don't want to be recorded.

If you have the following cyber security card, you don't need to take further action:

Unplug devices when not in use

You are used to having the device on only when you are actively using it.

If you don't have the card:

Skip a turn as you set up reminders to switch off the device every time you work on the project.

Threat: Your house is burgled. Your smartphone has been taken. You use your smartphone to connect apps to your device.

If you have the following cyber security card, you don't need to take further action:

Access codes for device apps

Your device cannot be used by people who don't have the access code.

If you don't have the card, roll the dice:

Odd Number: Thankfully, nothing seems to have happened.

Even Number: There are £100 of purchases made through your device. Pay £100. Move all Purchase Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

Threat: A friend gives you a USB stick with a game on it. As you plug it in to your laptop, you realise there's a virus on there.

If you have the following cyber security card, you don't need to take further action:

Use anti-virus software

The anti-virus software will stop the virus infecting your computer and the wider network.

If you don't have the card, roll the dice:

Odd Number: Pay £50 to have a professional come to check your entire network for viruses.

Even Number: Thankfully, nothing seems to have happened, aside from needing to reformat your laptop: skip a turn, or pay £10 to get someone else to do it for you.

Threat: Your device is acting strangely. You decide to Google for an answer, and settle on following the steps of a YouTube video that you found funny.

Did the solution suggested in the video fix the device? Roll the dice to find out...

Odd Number: It worked!

Even Number: It did not work, and now your device is unusable. Pay £100 to replace your device.

Outside Threat Card

Threat: Your device has been targeted by cyber criminals: if it still uses the default password it came with, it can be used by them to force websites offline.

Roll the dice:

Odd Number: You changed the password when you set up the device, so it's fine.

Even Number: Your Internet Service Provider notices that your device is acting maliciously and bars you from their service. Pay £100 to connect to a new ISP. Move all Connecting Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

Threat: Your device has a weakness in its software. A cyber criminal tries to access personal details on your computer through using the weakness in the device.

If you have the following cyber security card, you don't need to take further action:

Use your devices on a guest network

Your devices are on a separate network from your computer, which means the cyber criminal can't use the weakness to find the personal details.

If you don't have the card:

Skip a turn as you try to understand what's happened, or pay £10 to get someone else to do it for you.

The cyber criminal takes copies of all your data. Move all Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

Threat: A power surge has fried your device: it no longer works. You decide to buy a cheaper version from a different manufacturer, and buy a subscription to a new streaming platform that comes discounted with it.

Roll the dice:

Odd Number: You remember to close down the account with your previous streaming service, and request that they delete your data.

Even Number: You don't close down your old account. The old streaming service suffers a data breach, and your credit card details are stolen – and used. Move all Purchase Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

Threat: A streaming platform you use on your device has data stolen, and password information has been sold online.

Move all Streaming Data cards in your Manufacturer box to the Unwillingly Exposed Data box.

If you have the following cyber security card, you don't need to take further action:

Password manager

Your password is unique – you can change it and it should cause no further harm.

If you don't have the card:
Skip a turn to change your passwords.

Threat: Your smartphone has been stolen.

Buy a new smartphone for £100.

If you have the following cyber security card, you don't need to take further action:

Use a passcode on your smartphone

The person who has stolen your smartphone will need the passcode to use your profile.

If you don't have the card:

Skip a turn as you change all the passwords to your accounts.

Threat: You read that your device has a weakness that enables people to take a copy of the search histories performed on the devices, if the latest version of the software isn't installed.

If you have the following cyber security card, you don't need to take further action:

Switch on automatic software updates

Your device will have automatically installed the patch that fixes the weakness.

If you don't have the card:

Move all Search Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

Threat: The news reports that a group of cyber criminals have found a weakness in your device that enables them to record video and take pictures using the camera.

If you have the following cyber security card, you don't need to take further action:

Tape/sticker over camera

The tape/sticker is a physical barrier to stop anyone using the camera when you don't want them to.

If you don't have the card:

Skip a turn to find the recommended instructions from the manufacturer to avoid being recorded on camera, or pay £10 to get someone else to do it for you.

Threat: A malicious hacker decides to scare children by talking to them through devices on insecure networks.

If you have the following cyber security card, you don't need to take further action:

Change your router password

As your router password isn't the default one, the hacker can't get access.

If you don't have the card, roll the dice:

Odd Number: You aren't targeted, simply because there are too many other insecure devices he can choose from before yours.

Even Number: The hacker gains access and talks to your family. Skip a turn to change device and router password, or pay £10 to get someone else to do it for you. Move all Connecting Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

Threat: Your device manufacturer announces that they have just been made aware they had a data breach 5 years ago.

If you have this cyber security card, you don't need to take further action:

Data breach monitoring

You will be alerted if your data is discovered online.

If you don't have the card, roll the dice:

Odd Number: You notice fraudulent activity on your credit card. Skip a turn to go through it with the bank, or pay £10 to get someone else to do it for you.

Even Number: You don't notice anything unusual.

Threat: Your device manufacturer goes out of business. Effective immediately, they are unable to provide support for your device. You decide to keep using the device for as long as possible.

Roll the dice:

Odd Number: You continue to use the device. Some features no longer work.

Even Number: Newly discovered weaknesses in the device's software are targeted by cyber criminals. They take copies of all the data. Move all Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

Threat: Someone accesses your email account and password for your device.

If you have this cyber security card, you don't need to take further action:

Use an authenticator app with your devices

Without having access to the authenticator app, they cannot log into the device.

If you don't have the card:

Skip a turn as you get your account back, or pay £10 to get someone else to do it for you. Move all Data cards in your Manufacturer box to the Data Exposed Without Your Agreement box.

Quiz Card

Question: How does the UK's National Cyber Security Centre recommend you create strong passwords?

A) Use a long string of letters and numbers and symbols and never write them down.

B) Choose three random words and use them as one long pass phrase.

C) Use a base password, and alter it slightly for each account.

D) Use a password manager.

If team answers correctly:
Pick a new cyber security card.

Answer: B or D (either or both is fine!)

Question: How might you set up your home network to separate your home IoT devices from your smartphones and computers?

A) Using your router to create a guest network.

B) Get a second Internet connection in the house.

C) Connect smartphones and laptops to the Internet with mobile data only.

If team answers correctly:
Pick a new cyber security card.

Answer: A

Question: We have come up with 19 possible pieces of data a cyber criminal might want to get from your from your device. How many can you guess?

- Name
- Date of Birth
- Physical Address
- Account name
- Account password
- Other passwords
- Credit card details
- Device information
- Family information
- Device (IP) address
- Voice recordings
- Video recordings
- Search history
- Purchasing history
- Contacts
- Chat/message history
- Home routine
- Employment/school info
- Demographic info (e.g. info on your income, gender

If team answers:
1-5: win £5, 6-10: win £15, 11-15: win £30, 16 or more: win £50

Question: How old do you have to be to have an account on most platforms and all social media sites in the UK?

A) 5

B) 10

C) 13

D) 16

If team answers correctly:
They get to roll again.

Answer: C

Question: Can you describe five ways that free apps typically make money?

Give a point for each bullet point mentioned:

- Might collect data about the user
- Might collect data about the device
- Might sell data collected to third parties
- Might encourage users to buy things within the service/app
- Might limit free functionality and require users to pay to upgrade

If team answers:
1: win £5, 2-3: win £10, 4-5: win £20

Question: How might a ransomware attack on your device's manufacturer affect your device?

A) Device may no longer be able to do anything on the Internet.

B) You might not be able to access any account information.

C) Your personal data may be stolen and given to others without your permission.

D) There may not be any effect.

E) All of the above are possible.

If team answers correctly:
Pick a new cyber security card.

Answer: E

Question: Is performing a factory reset enough to delete all your data associated with a device?

A) Yes

B) No

If team answers correctly:
Pick a new cyber security card.

Answer: B – factory reset will wipe data from the device, but will not delete any other data stored by the manufacturer linked to your account.

Question: Can you give two main reasons why apps need updating on devices?

Give a point for each bullet point mentioned:

- When bugs are found, software needs to be updated to fix them.
- When new features are designed or the device needs to do new things, software needs to be updated to include them.

If team answers:
1: win £5, 2: win £15

Question: What five steps should you take before you sell or get rid of a device?

Give a point for each bullet point mentioned:

- Back up any important data.
- Make sure you know if the device links to any other accounts, and how you will manage this once you don't have the device.
- Perform factory reset.
- If necessary, close your account.
- If necessary, ask manufacturer to delete your data.

If team answers:
1: win £10, 2: win £10, 3 or more: win £20

Question: Which government organisation is responsible for giving UK citizens advice for protecting themselves when using technology?

A) Department for Education

B) National Cyber Security Centre

C) Cabinet Office

D) National Crime Agency

If team answers correctly:
They get to roll again.

Answer: B

Question: How long does a typical smartphone receive automatic software updates ?

A) Android 2-3 years, Apple 5-6 years

B) Android 6-7 years, Apple 4-5 years

C) Android 1-2 years, Apple 2-3 years

If team answers correctly:
They get to roll again.

Answer: A

Cyber Security Card

Back up devices

Backing up data allows it to be available, even if something goes wrong with the device.

Cost: £5 (when first picked up then each time around the board)
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
If important data is backed up in a safe place, it should remain accessible in an emergency

Con
Hard to access data from smart devices
Harder to put data back into smart devices

Tape/sticker over cameras

You can put something, like dark tape or a post-it note, over a camera that does not have its own cover to ensure that no-one can watch in without it being removed.

Cost: None
Time to set up: None

Pro
It's a very low-tech, easy solution

Con
It may be tricky to see where the cameras are in some devices

Data breach monitoring

If your data is taken in a data breach, there are services that can inform you of this, so that you can take steps (change passwords, be very careful of any odd looking emails) to protect your identity.

Cost: None
Time to set up: None

Pro
If informed your information has been breached, you can take action

Con
You will only find out if the breach is made public

Access codes for device apps

Even if someone accesses your smartphone, they will need to know the code to use apps associated with devices.

Cost: None
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
It's an extra level of security

Con
Forgetting it would make it difficult to access your account

Profiles for devices

Devices can often allow for multiple profiles to be set up to enable different types of access.

Cost: None
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
Each user can have their own settings and passcodes

Con
Can be difficult to juggle many profiles

Unplug devices when not in use

You can turn devices off when they are not being used. Some devices may also offer a muting function.

Cost: None
Time to set up: None

Pro
You control when the device is on

Con
It's difficult to remember to do this

Devices are not designed to work like this

Family discussion: device use

Research has shown that families that agree on common rules about device use ahead of time do better at sticking to them.

Cost: None
Time to set up: Skip a turn

Pro
Better device understanding

You decide on what works for you all

Con
Everyone needs to agree

Password manager

Software to generate and save strong and unique passwords.

Cost: £5 (when first picked up then each time around the board)
Time to set up: None

Pro
Generate and save unique passwords for every account

Con
You have to pay for a subscription

You have to have the password manager on all your devices, or you won't be able to log in

Change your router password

Your router's password is typically printed on the side of the device, so could be seen by many people. Changing the password will make it less likely that people you don't want will access it.

Cost: None
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
Makes accessing the network harder

Con
It can feel quite technically hard to do this

Use your devices on a guest network

Some routers can provide two wifi networks, allowing you to put home IoT devices on a different network to computers and phones.

Cost: None
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
This can protect devices from malware (like viruses) introduced through computers or phones (on the other network)

Con
It can be tricky to set up

Devices are not designed to work like this

Use an authenticator app with your devices

An authenticator app creates codes for you to use, in addition to user name and password, when logging into an account.

Cost: None
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
This is an additional layer of defence compared to just having a password

Con
You need your phone nearby

Set up can be tricky and take a little time

Turn off automatic purchases on your device

Some devices tend to be sold with settings enabling people to buy products through the device switched on by default.

Cost: None
Time to set up: None

Pro
Turning off these settings will avoid unexpected purchases

Con
Devices work better with all features switched on

Use anti-virus software

Software that scans your device (typically a computer, sometimes they can be used on smart phones and smart TVs) looking for files that it knows to be malicious (e.g. viruses).

Cost: £5 (when first picked up then each time around the board)
Time to set up: None

Pro
It will help to stop the device it is used on being infected

Con
You have to pay a subscription

Anti-virus does not necessarily work on all devices

Switch on automatic software updates

Setting software to update automatically allows your system to install patches and upgrades when available.

Cost: None
Time to set up: None

Pro
Once switched to automatically update, you don't have to do anything

Con
You might not realise when your device stops being updated

Review devices on your network

Devices don't usually forget networks once they have connected. Reviewing devices occasionally allows to you remove devices you don't want on the network.

Cost: None
Time to set up: Skip a turn, or pay £10 to get someone else to set it up for you

Pro
Confirmation that no one/no device has unexpected access to the network

Con
Can be a technical process

Will need change the network password as well if unexpected devices are found

Use a passcode on your smartphone

Your smartphone is the key to a significant amount of personal data. Use a pin, passcode, or biometric data (face recognition, fingerprint) to access it.

Cost: None
Time to set up: None

Pro
It makes accessing the phone harder

Con
You have to remember the code

Regularly delete device histories

Data collected by devices can typically be deleted, thus making it unavailable to anyone.

Cost: None
Time to set up: None

Pro
The less data a device has, the less there is to be lost, stolen or otherwise used badly

Con
The device may often need significant data to offer smart insights or personalisation

Data Card: Connecting data

Connecting data

Information you might share when you connect to a device with your smartphone

Your smartphone make, model, software details

Your unique device address

Other devices on your home network

Data Card: Streaming data

Streaming data

Information you might share when you stream media using software on a device

Your account profile data

Your streaming history

Recommended future streaming based upon your past streaming activity

Data Card: Search data

Search data

Information you might share when you search for information using software on a device

Your search history

Your video/video recordings

Your profile based upon previous searches

Data Card: Purchase data

Purchase data

Information you might share when you purchase something using a device

Your home address

Your credit card details

Recommended future purchases based on your past shopping

Appendix I

Content and explanation of scenario and cyber security tool cards

Content explanation

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Inside Threat	Someone in the house has tried to use your smartphone.	Access codes for device apps.	“Some devices may be insecure when they are first switched on, so you’ll need to take some quick steps to protect yourself.” `https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home`
Inside Threat	Someone in the house has tried to buy something through your device.	Turn off automatic purchases on your device.	“Mum hit with huge Amazon bill as daughter, 5, orders diamond necklace and £300 of same Disney toy” `https://www.mirror.co.uk/news/uk-news/mum-hit-huge-amazon-bill-11438787` and evidence from initial interview participants
Inside Threat	A relative visits your home, and when looking at your device, presses some buttons, and some settings get deleted.	Profiles for devices. (Skip a go)	“I deleted devices and home by accident!” SmartThings community forum `https://community.smartthings.com/t/i-deleted-devices-and-home-by-accident/145013/8`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Inside Threat	One of the children in the house has accessed content you're not happy with on your device.	Family discussion: device use	"Alexa tells 10-year-old girl to touch live plug with penny" `https://www.bbc.co.uk/news/technology-59810383` and following research from Ko et al. (2015) and Blum-Ross and Livingstone (2020).
Inside Threat	Someone has decided to play a joke on you by modifying the settings on your device.	Use an authenticator app with your devices	"If the device or app offers two-factor authentication (2FA), **turn it on** [sic]. 2FA provides a way of 'double-checking' that you really are the person you are claiming to be." `https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home`
Inside Threat	You have a serious falling out with a neighbour who has, in the past, connected to your home Wi-Fi with their laptop and phone.	Review devices on your network	Following research presented at BlackHat: Hacking A Capsule Hotel `https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Hacking-A-Capsule-Hotel-Ghost-In-The-Bedrooms.pdf` and "If someone else gains access to that network—whether a remote hacker or your next-door neighbour—it can be quick work to compromise those devices." `https://www.wired.com/story/secure-your-wi-fi-router/`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Inside Threat	A friend of the youngest member of the family takes too much of an interest in your device. They are too young to understand how to use the device properly and accidentally delete some data.	Back up devices.	`https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data`
Inside Threat	You need to do a project at home, that requires talking to lots of people over videochat about quite sensitive things you don't want to be recorded.	Unplug devices when not in use.	Following research from Dubois et al. (2020) and advisories from firms such as Mischon de Reya to turn off or mute devices when working `https://www.telegraph.co.uk/technology/2020/03/30/lawyers-urged-switch-alexa-working-home/`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Inside Threat	Your house is burgled. Your smartphone has been taken. You use your smartphone to connect apps to your device.	Access codes for device apps	"Some devices may be insecure when they are first switched on, so you'll need to take some quick steps to protect yourself." https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home
Inside Threat	A friend gives you a USB stick with a game on it. As you plug it in to your laptop, you realise there's a virus on there.	Use antivirus software.	" Your devices can become infected by inadvertently downloading malware that's in an attachment linked to a dubious email, or hidden on a USB drive, or even by simply visiting a dodgy website." https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product
Inside Threat	Your device is acting strangely. You decide to Google for an answer, and settle on following the steps of a YouTube video that you found funny.	N/A	Evidence from initial interview participants and the Cyber Security Awareness Information Review.

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Outside Threat	Your device has been targeted by cyber criminals: if it still uses the default password it came with, it can be used by them to force websites offline.	N/A	“Some devices may be insecure when they are first switched on, so you’ll need to take some quick steps to protect yourself.” `https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home`
Outside Threat	Your device has a vulnerability in its software. A cyber criminal tries to access all your devices on the same network, including computers and phones, through this vulnerability.	Use your devices on a guest network	“Secure your network. Your fridge and your laptop should not be on the same network. Keep your most private, sensitive data on a separate system from your other IoT devices.” `https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Outside Threat	A power surge has fried your device: it no longer works. You decide to buy a cheaper version from a different manufacturer, and buy a subscription to a new streaming platform that comes discounted with it.	N/A	"Having too many digital accounts raises your risk of data being misused or stolen." `https://www.consumerreports.org/privacy/how-to-delete-online-accounts-you-no-longer-need-a1194263953/`
Outside Threat	A streaming platform you use on your device has had a data leak, and passwords have been leaked.	Password manager	"A password manager ... can store all your passwords securely, so you don't have to worry about remembering them. This allows you to use unique, strong passwords for all your important accounts." `https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Outside Threat	Your smartphone has been stolen.	Use a passcode on your smartphone.	“Screen locks offer your devices an important extra layer of security.” `https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/secure-your-tablet-or-smartphone-with-a-screen-lock`
Outside Threat	You read that your device has a vulnerability that enables people to take a copy of the search histories performed on the devices, if the latest version of the software isn’t installed.	switch on automatic software updates.	“As with your computers and smartphones, installing software updates promptly helps keep your devices secure.” `https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Outside Threat	The news reports that a group of cyber criminals have found a vulnerability in your device that enables them to record video and take pictures using the camera.	"If you can't turn off a camera but want to – a simple piece of black tape over the camera eye is a back-to-basics option." https://flashalert.net/id/FBIOregon/129449	
Outside Threat	A malicious hacker decides to scare children by talking to them through devices on insecure networks.	Change your router password	"A Mississippi family said someone hacked a Ring security camera set up in their children's bedroom and taunted their 8-year-old daughter." https://www.nbcnews.com/news/us-news/man-hacks-ring-camera-8-year-old-girl-s-bedroom-n1100586

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Outside Threat	Your device manufacturer announces that they have just been made aware they had a data breach 5 years ago.	Data breach monitoring	“Now would also be a good time to check if your account has appeared in any other public data breaches. Visit `https://haveibeenpwned.com`, enter your email address and go from there.” `https://www.ncsc.gov.uk/guidance/ncsc-advice-british-airways-customers`
Outside Threat	Your device manufacturer goes bust. Effective immediately, they are unable to provide support for your device. You decide to keep using the device for as long as possible.	N/A	“As with your computers and smartphones, installing software updates promptly helps keep your devices secure.” `https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home` and following evidence from initial interview participants.
Outside Threat	Someone accesses your email account and password for your device.	Use an authenticator app	“If the device or app offers two-factor authentication (2FA), **turn it on** [sic]. 2FA provides a way of ’double checking’ that you really are the person you are claiming to be.” `https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Cyber Security Tool	Back up devices	N/A	“As a rule of thumb, **you should back up anything that you value** [sic].” https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data
Cyber Security Tool	Tape/sticker over cameras	N/A	“If you can’t turn off a camera but want to – a simple piece of black tape over the camera eye is a back-to-basics option.” https://flashalert.net/id/FBIOregon/129449
Cyber Security Tool	Data breach monitoring	N/A	“Now would also be a good time to check if your account has appeared in any other public data breaches. Visit https://haveibeenpwned.com, enter your email address and go from there.” https://www.ncsc.gov.uk/guidance/ncsc-advice-british-airways-customers
Cyber Security Tool	Access codes for device apps	N/A	“Some devices may be insecure when they are first switched on, so you’ll need to take some quick steps to protect yourself.” https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Cyber Security Tool	Profiles for devices	N/A	“If you provide a connected device then you need to pay attention to the potential for it to be used by multiple users of different ages. This is particularly the case for devices such as home hub interactive speaker devices which are likely to be used by multiple household members, including children, and may also be used by visitors to the home.” `https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/14-connected-toys-and-devices/`
Cyber Security Tool	Unplug devices when not in use	N/A	Following research from Dubois et al. (2020) and advisories from firms such as Mischon de Reya to turn off or mute devices when working `https://www.telegraph.co.uk/technology/2020/03/30/lawyers-urged-switch-alexa-working-home/`
Cyber Security Tool	Family discussion: device use	N/A	Following research from Ko et al. (2015) and Blum-Ross and Livingstone (2020).

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Cyber Security Tool	Password Manager	N/A	“A password manager ... can store all your passwords securely, so you don’t have to worry about remembering them. This allows you to use unique, strong passwords for all your important accounts.” https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
Cyber Security Tool	Change your router password	N/A	“...it’s essential to keep your router secure.” https://www.wired.com/story/secure-your-wi-fi-router/
Cyber Security Tool	Use your devices on a guest network	N/A	‘Secure your network. Your fridge and your laptop should not be on the same network. Keep your most private, sensitive data on a separate system from your other IoT devices.” https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot
Cyber Security Tool	Use an authenticator app with your devices	N/A	“If the device or app offers two-factor authentication (2FA), **turn it on** [sic]. 2FA provides a way of ’double-checking’ that you really are the person you are claiming to be.” https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Cyber Security Tool	Turn off automatic purchases on your device	N/A	"Mum hit with huge Amazon bill as daughter, 5, orders diamond necklace and £300 of same Disney toy" `https://www.mirror.co.uk/news/uk-news/mum-hit-huge-amazon-bill-11438787` and evidence from initial interview participants
Cyber Security Tool	Use antivirus software	N/A	"...it's important that you always use antivirus software, and keep it up to date to protect your data and devices." `https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product`
Cyber Security Tool	Switch on automatic software updates	N/A	'As with your computers and smartphones, installing software updates promptly helps keep your devices secure." `https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Cyber Security Tool	Review devices on your network	N/A	Following research presented at BlackHat: Hacking A Capsule Hotel `https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Hacking-A-Capsule-Hotel-Ghost-In-The-Bedrooms.pdf` and “If someone else gains access to that network — whether a remote hacker or your next-door neighbour — it can be quick work to compromise those devices.” `https://www.wired.com/story/secure-your-wi-fi-router/`
Cyber Security Tool	Use a passcode on your smartphone	N/A	‘Screen locks offer your devices an important extra layer of security.” `https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/secure-your-tablet-or-smartphone-with-a-screen-lock`

Continued on next page

Type of Card	Text on Card	Tool for Mitigation	Explanation for inclusion
Cyber Security Tool	Regularly delete device histories	N/A	“If you haven’t been regularly deleting your voice history with Amazon’s voice assistant, Alexa, you could have a good reason to start: a recently fixed vulnerability that would’ve exposed all your conversations with the smart speaker.” `https://www.cnet.com/home/smart-home/alexa-vulnerability-is-a-reminder-to-delete-your-voice-history/`

Appendix J

Pre-game survey questions — both non-control and control groups

J.1 Key to questions

Questions with a filled bullet point denote a single response question.
Questions with an empty bulletpoint denote that multiple choices are possible in an answer.
Every "other" option has a text box that must be populated if chosen.
All questions are mandatory.

J.2 Household Information

How many adults (18+) live in your house? (choose one)

- 1
- 2
- 3
- 4
- 5
- 6+

What is/are the age ranges of child(ren) in your house? (choose all applicable) *[checklist range from 0-18]*

J.3 Devices

What devices do you currently own or have in your household?

- ○ Connected alarm system
- ○ Connected baby monitors
- ○ Connected children's toys
- ○ Connected door lock
- ○ Connected doorbell
- ○ Connected fridge/freezer
- ○ Connected heating or air conditioning unit
- ○ Connected home automation system
- ○ Connected smoke detector
- ○ Connected thermostat
- ○ Connected washing machine/tumble dryer
- ○ Other connected safety-relevant product
- ○ Other smart kitchen appliance
- ○ Other smart personal hygiene device
- ○ Robot cleaner
- ○ Smart camera
- ○ Smart home assistant (sometimes referred to as smart speaker)
- ○ Smart kitchen appliance
- ○ Smart lighting
- ○ Smart meter
- ○ Smart plugs
- ○ Smart printer

- Smart scale
- Smart toothbrush
- Smart TV
- Smart vacuum
- Streaming device (typically connects a smartphone to TV, e.g. Chromecast, Fire Stick)
- Other device type not listed

Do you take responsibility for the majority of decisions around device purchase and management in the home?

- Yes
- No, another adult in the house does
- No, a child in the house does (give age of child)

J.4 Smart TV/Streaming Device/Smart Home Assistant use

How often do you use the smart features (i.e. features that require you to be connected to the Internet) on your smart TV and/or home assistant a week?

Smart TV:

- Every day
- 4-5 days of the week
- 2-3 days of the week
- Once a week
- Less frequently
- n/a

Streaming device:

- Every day

- 4-5 days of the week
- 2-3 days of the week
- Once a week
- Less frequently
- n/a

Smart home assistant:

- Every day
- 4-5 days of the week
- 2-3 days of the week
- Once a week
- Less frequently
- n/a

Does your family use paid for services/apps/skills on your devices (e.g. streaming services such as Netflix or Amazon Prime)?

Smart TV:

- Yes, 5+
- Yes, 3-4
- Yes, 1-2
- No
- n/a

Streaming Device:

- Yes, 5+
- Yes, 3-4
- Yes, 1-2
- No
- n/a

Smart home assistant:

- Yes, 5+
- Yes, 3-4
- Yes, 1-2
- No
- n/a

Does your family use free services/apps/skills on your devices (e.g. streaming services or apps)?

Smart TV:

- Yes, 5+
- Yes, 3-4
- Yes, 1-2
- No
- n/a

Streaming Device:

- Yes, 5+
- Yes, 3-4
- Yes, 1-2
- No
- n/a

Smart home assistant:

- Yes, 5+
- Yes, 3-4
- Yes, 1-2
- No
- n/a

Thinking about the majority of the services you use on these types of smart devices, do they give you the option to set up profiles for your family members?

- Yes, all of them do
- Yes, more than half of them do
- Yes, fewer than half of them do
- No, none do
- I don't know

Do you take advantage of separate profiles for family members where available?

- Yes, for all accounts with the option
- Yes, for some of the accounts with the option
- Yes, for one of the accounts with the option
- No, we do not use this feature when offered
- I don't know

Smart TVs, streaming devices and smart home assistants can collect significant amounts of data about their users; some of these data types are listed below. Looking at this list, rank the data types you would consider the most important to keep safe from those people or organisations you don't want to give it to. Rank from 1 (most important) to 10 (least important): each data type must have a different rating.

- Account log in details
- Account usage information (e.g. voice recordings, video recordings, usage history, public and private communication/messaging history, search histories, purchase history)
- Biometric data (e.g. fingerprints, voice signature, facial recognition data)
- Contact information (e.g. e-mail addresses, home addresses, phone numbers)
- Demographic info (including information on age, sex, gender identity, race, ethnicity, employment, income levels, marital status, education levels, religious affiliation) of people in the household

- ○ Device information (e.g. IP addresses, IMEI numbers, operating system information)
- ○ Financial information (e.g. credit card details, debit card details, banking information)
- ○ Network information (e.g. type of router, Internet Service Provider used, devices connected to the network, firewall set up)
- ○ Passwords
- ○ Personal information (e.g. names of users, date of birth, place of birth)

Were there any other data types not mentioned here that you are aware of providing your smart TV, streaming device or smart home assistant? Detail below, and provide an explanation of how important it is to keep that data type to keep safe from those people or organisations you don't want to give it to.

[Free text answer]

J.5 Cyber security

When you think about the potential for the misuse of smart TVs, streaming devices or smart home assistants that you own or use, whom are you most concerned about? Choose up to 3.

- ○ Adults within the house
- ○ Children within the house (give age(s) of children you are concerned about)
- ○ Device manufacturers
- ○ External malicious parties (e.g. hackers, criminals)
- ○ Other family members with access to your network
- ○ Other occasional visitors (tradespeople, cleaners, carers, childcare etc)
- ○ People who have access to your network but do not live with you (e.g. friends, neighbours)
- ○ The government (your own or other country)
- ○ Yourself

○ Your Internet Service Provider

○ Other

Can you give a reason?
[Free text answer]

When you think about the potential for the misuse of the smart TV(s), streaming device(s) or smart home assistant(s)that you own or use, what are you most concerned about? Choose up to 3.

○ Corporate/company/school/organisation financial loss

○ Financial fraud

○ Inability to perform core tasks (e.g. work, schooling, keeping family safe and healthy)

○ Inability to solve the problem

○ Inability to use devices

○ Inability to use home network setup as intended

○ Loss of access to services

○ Other financial loss (such as inability to use subscription services)

○ Personal data leak

○ Personal data loss

○ Physical harm to device

○ Physical harm to individuals

○ Physical harm to other things

○ Other

Can you give a reason?
[Free text answer]

Which of these measures do you currently use to protect your smart TV(s) and/or streaming devices and/or smart home assistant(s) on your home network? Click all that apply.

- ○ Back up important data
- ○ Change default passwords to strong, unique passwords
- ○ Disable UPnP and port forwarding on your router
- ○ Discuss appropriate device use with other home users
- ○ Limit privileges or change default permissions
- ○ Limit sensitive data stored in the cloud
- ○ Limit sensitive data stored in the device/supporting apps
- ○ Not using unsupported devices
- ○ Performing factory reset when getting rid of your device
- ○ Put a cover over cameras attached to devices
- ○ Regularly delete usage history
- ○ Regularly update software
- ○ Save/store passwords (in device, in password manager, in offline/physical notebook)
- ○ Use a virtual private network (VPN)
- ○ Use antivirus software
- ○ Use two-factor authentication
- ○ Using a guest network
- ○ Other

Which of these security options have you heard of but do not use?

- ○ Back up important data
- ○ Change default passwords to strong, unique passwords
- ○ Disable UPnP and port forwarding on your router
- ○ Discuss appropriate device use with other home users
- ○ Limit privileges or change default permissions
- ○ Limit sensitive data stored in the cloud

- ○ Limit sensitive data stored in the device/supporting apps
- ○ Not using unsupported devices
- ○ Performing factory reset when getting rid of your device
- ○ Put a cover over cameras attached to devices
- ○ Regularly delete usage history
- ○ Regularly update software
- ○ Save/store passwords (in device, in password manager, in offline/physical notebook)
- ○ Use a virtual private network (VPN)
- ○ Use antivirus software
- ○ Use two-factor authentication
- ○ Using a guest network

Can you explain why for any or all of the selected answers?

[Free text answer]

Appendix K

Pre-game questionnaire

This appendix shows the pre-game questionnaire provided to participating families at the start of the gameplaying session, to be filled out by each team.

University of Kent

Pre-game device considerations
(one per team)

What is worth protecting on our smart TV/streaming device/smart home assistant?

Who do we want to protect it from, and how likely are we going to have to protect it from them?

How bad is it if we fail?

What do we currently do to avoid this happening?

Do we all do the same things?

Appendix L

Post-game questionnaire

This appendix shows the post-game questionnaire provided to participating families at the end of the gameplaying session, to be filled out by the family as a group.

Post-game device considerations
(one for the entire family)

University of Kent

What is worth protecting on our smart TV/streaming device/smart home assistant?
Who do we want to protect it from, and how likely are we going to have to protect it from them?
How bad is it if we fail?
Are we going to do anything new to stop this from happening?
What do we all agree to do to keep the devices safer?

Appendix M

Post-game interview questions

These questions are asked to each family player individually, children first, with language modified for younger children):

- How did you think playing the game went?
- What elements did you enjoy?
- Did you learn anything when playing the game?
- What elements didn't you enjoy?
- Were there any parts of the game where you needed support from other family members? Can you remember why?
- Was there anything that left you confused, or feeling like you didn't understand what was being said?
- Were there any parts of the gameplay that you would see changed, removed, or added?
- Were there any parts of the written aspects (the instructions, the cards) that you would see changed, removed, or added?
- Do you have any thoughts of the look and feel of the game? What would you change? Which colours and types of graphics would you use?
- Do the cards and pieces used in the gameplay feel appropriate to you? Would you change, remove, or add anything?

- Have you done any work or training or anything else related to the topics covered by the game in the last week? What happened there, and did you see overlaps with the choices and options in the game?
- Do you think the gameplay took the right amount of time?
- Were there the right amount of boxes around the board?
- Do you think that the amount of money used throughout the game was sufficient for what you had to do with it?
- Did the way you had to use the money make sense to you?
- Did the data cards make sense to you?
- Did the cyber security tools cards make sense to you?
- Were there any of the Internal, External Threat or Quiz cards that particularly made you think? Or any that you did not understand or would remove?
- Are there other smart home devices that you might have felt this game would work better with?
- Will you be taking any learning home today to put into practice?
- Were there any scenarios, questions or tools that you did not understand the point of, that you would never consider applying to your life or that otherwise didn't seem useful?
- Did you write down any other notes or ideas as you were playing the game that we haven't discussed yet?

Appendix N

Post-game survey questions — non-control, then control groups

N.1 *

Key to questions

Questions with a filled bullet point denote a single response question.
All questions are mandatory.

N.2 *

Non-control group survey Do you and your family have any more thoughts or comments that could help further development of the game that you played with us the other day?

[Free text answer]

Please rate the following phrases from 1-5 (1 being the least, 5 being the most):

- We enjoyed playing the game
- We learned about device use because of playing the game
- We learned about cyber security because of playing the game
- We discussed device use as a family because of playing the game
- We discussed cyber security as a family because of playing the game

Have you received any other training, or been exposed to anything else (e.g. news articles, TV shows) since you played the game that had the intention of helping you understand cyber security or home IoT devices better?

[Free text answer]

If you decided, as a family, to implement new or different security solutions, has that happened? Have you encountered any problems?

[Free text answer]

Are you aware of any data breaches or cyber security stories in the news since you played the game? If so, which?

[Free text answer]

Have you bought any other home IoT devices since you played the game? If so, which?

[Free text answer]

N.3 *

Control group survey

Have you received any training (e.g. in a work, educational or voluntary context), or been exposed to any other sources of information (e.g. news articles, TV shows) since answering the first survey that had the intention of helping you understand cyber security or home IoT devices better?

[Free text answer]

Have you decided to implement new or different cyber security solutions for the home IoT devices in your home since answering the first survey? Have you had any difficulties doing this? Did anything specifically prompt this?

[Free text answer]

Are you aware of any data breaches or cyber security stories in the news since you answered the first survey? If so, which?

[Free text answer]

Have you bought any other home IoT devices since you filled in the first survey? If so, which?

[Free text answer]

Appendix O

Game interviews code book

Game Interviews Code Book

Top-level code	Second-level code	Sub codes
Cyber security		
	Known cards/known cyber security solutions	
		Round three
		Round two
		Round one
	Family discussion during session	
		Round three
		Round two
		Round one
	Unknown cards/unused cyber security solutions	
		Round three
		Round two
		Round one
	Cyber security knowledge children	
		Round three
		Round two
		Round one
	Cyber security knowledge adult	
		Round three
		Round two
		Round one
Participatory Design		
	Improvement between Round 1 to 2	
		Round two
	Game confusion	
		Round three
		Round two
		Round one
	Game dislikes	
		Round two
		Round one
	Game likes	
		Round three
		Round two
		Round one
	Gameplay	
		Round three
		Round two
		Round one
	Design	
		Round two
		Round one
	Cards	
		Round three
		Round two
		Round one
	Board and Pieces	
		Round two
		Round one

Appendix P

Information booklet

This chapter includes the information booklet given to game participants alongside the game.

What does that mean?

A Guide To Some of the Terms in the Game

University of Kent
Institute of Cyber Security for Society (iCSS)

Term	Explanation
Access code	A short combination (usually 4 or 6 digits) that have to be entered in order to access an app. May also be referred to as a PIN.
Account	An account is an identity created for a person in a computer or computing system. An account may enable the creation of several profiles within it.
Anti-virus (anti-malware) software	Anti-virus software is a computer program used to prevent, detect, and remove viruses (malware). It can be used on computers and smartphones, and some Internet of Things devices. For more information, you can read the NCSC's pages on anti-virus here: https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product
App	An app is a piece of software typically designed to run on a mobile device, such as a smartphone, tablet or smartwatch.
Authenticator App	Authenticator apps generate a one-time code that you use to confirm that it's you logging in to a website or service; they provide the second part of what's called two-factor authentication (2FA). They are considered to be more secure than receiving SMS codes. There are many options of Authenticator apps, based on things like the smartphone operating system you have, as well as personal preference. For more, you can read Which?'s guidance here https://computing.which.co.uk/hc/en-gb/articles/360006153539-How-to-set-up-an-authenticator-app-for-two-factor-authentication, or the NCSC's guidance here: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email

University of Kent | Institute of Cyber Security for Society (iCSS)

Term	Explanation
Automatic software updates	Allowing software to update automatically (typically when it has a stable connection to the Internet) allows for fixes to weaknesses in the underlying code to be applied without you having to do anything. Such updates also will include new tools and features, so it is worth your while! Importantly, though, most software is only supported for a limited time, and will not receive updates - even important ones, in many cases - after that time. To read more, see the NCSC's page here: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates
Back up	A back up is a copy of (typically) important data that is stored in a separate, safe, location - often online (sometimes called cloud storage), or on removable media (such as a USB stick or external hard drive). If you lose the original data, the idea is that you can retrieve it from the back up location. To read more, see the NCSC's page here: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data
Biometric Data	Biometrics are body measurements and calculations related to human characteristics. Typically used in smart technologies are biometrics related to the face (facial recognition), or fingerprint (fingerprint recognition), but could also refer to voice recognition or gait (movement) recognition, for instance. These pieces of information will be "read" by the appropriate sensor type (a camera or microphone, for example), and, when used as a passcode, will be checked against a mathematical representation of that measurement to allow access.

Term	Explanation
Bugs	Software bugs are errors or faults in computer software that causes it to produce an incorrect or unexpected outcome. They are named, in part at least, after the account of computing pioneer Grace Hopper who discovered a moth trapped within a relay of the computer she was working with (the Mark II). The offending moth was removed, and taped to her logbook.
Cloud (storage)	"The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers. This is in contrast to running locally on your computer. Typically, individuals today will use a cloud service (such as Google Drive, Microsoft's Office 365/OneDrive, Apple's iCloud) to back up files.
Cyber security	Cyber security is the term given to the protection of computer systems and networks. This can be protection from unwanted information disclosure or theft, from damage to hardware, software or data or from disruption of services.
Data breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. You can read more about personal data breaches at the ICO's website here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatisa

Term	Explanation
Data breach monitoring	Data breach monitoring services are typically websites (although they can also be offered as part of password management tools) that track publicly disclosed data breaches. You provide details - typically an email address - to the service, and should that email address match with any confirmed leak of data, you will be notified (so that you can, at the least, assess whether you need to change a password or take further action). The most famous website, that works with several governments, is haveibeenpwned.com.
Default Password	A default password is a standard pre-configured password for a device. Such passwords are the default configuration for many devices and, if unchanged, present a serious security risk. Typical examples of default passwords include admin, password, 1234, and guest. You should check to see that any time you set up a new device, that the password is changed.
Device (IP) Address	An IP (or device) address is a network address for your computer or device so the internet knows where to send your data. IP stands for "Internet Protocol". Each address is unique, and is linked to the activity that happens online from that device.
Device/Search History	The search history of a device is a list of Internet activity (often, but not always, web pages) that a user has undertaken, along with additional information (called metadata) about the specifics of the visit (e.g. time of visit). Users can usually search through this history within apps or search engines, and should be able to delete details of the history within the app or search engine.
External Hard Drive	An external hard drive is a device that you plug into a computer; you can transfer data on to the external hard drive, then remove it. This is helpful as a means to backup.

Term	Explanation
Factory Reset	A factory reset is the restoration of a device to the state it was in when it left the factory. It is important to note that doing a factory reset affects the device, but will still keep data in accounts that are kept in the cloud.
Guest Network	A guest WiFi network provides an access point to the internet separate from the one your primary devices connect to. This is managed through your router.
Hardware	Hardware is the word used to refer to the physical aspect of a piece of technology. Hardware works because of the software that runs on it.
Information Commissioner's Office (ICO)	The Information Commissioner's Office is the UK's regulator for data protection. The Commissioner's mission is to "uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." You can find out more here: https://ico.org.uk/
Internet of Things	The Internet of things describes physical objects with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.
Internet Service Provider (ISP)	An Internet service provider is an organization that provides services for accessing, using, or participating in the Internet.
Interoperability	Interoperability is the ability of computer systems or software to exchange and make use of information. This is particularly important in internet of things devices, that often work together in a home (for example).

Term	Explanation
National Cyber Security Centre (NCSC)	The National Cyber Security Centre (NCSC) provides cyber security guidance and support helping to make the UK the safest place to live and work online. Find out more here: https://www.ncsc.gov.uk/
Network	A home network is a group of devices – such as computers, game systems, printers, and mobile devices – that connect to the Internet and each other, whether through wired connections or over wireless connections.
Password manager	A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services. To read more about what to consider when looking for a password manager, read more here: https://www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide
Personalisation	Personalisation is the process whereby the data that you are providing to a service is used to target other information to you - often to try and sell you more specific products.
Phishing	Phishing is a type of social engineering attack, typically involving a contact over email, in which cyber criminals trick victims into handing over sensitive information or installing malware.
PIN	A PIN (a personal identification number) can also be referred to as an access code. A PIN is a passcode used in the process of authenticating a user accessing a system.

Term	Explanation
Privacy	Privacy, in relation to personal data, is the ability of individuals to control their personal information.
Ransomware	Ransomware a type of malicious software designed to block access to a computer system until a sum of money is paid.
Removable Media	Removable media is a type of storage device that can be removed from a computer whilst the system is running. Examples include: USB memory sticks. External hard drives. They are good for use as a back up.
Router	A router is a device that communicates between the Internet and the devices in your home that connect to the Internet. As its name implies, it "routes" traffic between the devices and the Internet. It is very often the piece of hardware provided by your ISP when changing broadband providers, and is the piece of hardware that provides your WiFi connection. Some routers can also provide the ability to set up guest networks (although this depends on the router).
Smart Assistant	A smart assistant – also known as a virtual assistant – is software installed in a smart device (such as a smart speaker or a smart phone) that can perform tasks or services, or answer questions.
Smart Home	A smart home is a home setup where Internet-enabled appliances and devices can be automatically controlled remotely using a networked device (such as a smartphone).
Smart TV	A smart TV - also known as a connected TV - is a traditional television set with integrated Internet and interactive features, which allows users to stream music and videos, browse the internet and view photos.

University of Kent | Institute of Cyber Security for Society (iCSS)

Term	Explanation
Social engineering	Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.
Smishing	Smishing is a type of social engineering attack, typically involving a contact over SMS or text, in which cyber criminals trick victims into handing over sensitive information or installing malware.
Software	Software is a collection of instructions that tell a computer how to work.
Streaming (media)	Streaming media is multimedia that is delivered and consumed in a continuous manner from a source, typically over the Internet, with no storage on the device used to stream the multimedia.
Threat Model	Threat Modelling is a process of determining how to mitigate potential threats, and prioritise those mitigations. For more details on how to threat model in relation to personal data, see https://ssd.eff.org/en/module/your-security-plan.
Two/Multi-Factor Authentication (2FA, MFA)	Two, or Multi-Factor, Authentication is an authentication method that requires the user to provide two or more (multi) verification factors to gain access to a piece of software. Methods of authentication can include a combination of passwords, biometric data, physical tokens, authenticator apps, and one time codes.
USB Flash Drive	A USB flash drive (also called a thumb drive) is a data storage device. It is a type of removable media, and can be useful for saving back up data on.
Virus (Malware)	Malware (sometimes referred to as viruses - although, in fact, viruses are a subset of all malware) is intrusive software that is designed to damage and destroy computers and computer systems.

University of Kent

Institute of Cyber Security for Society (iCSS)

Term	Explanation
Vishing	Vishing is a type of social engineering attack, typically involving a contact over telephone calls or answerphone messages, in which cyber criminals trick victims into handing over sensitive information or installing malware.
Vulnerability (Weakness)	A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal. To read more, see: https://www.ncsc.gov.uk/information/understanding-vulnerabilities.

Appendix Q

Final game cards

This appendix provides the finalised game cards that were created for the third round of the game.

Inside Threat

Access smartphone

Access smartphone

You try to access the other team's devices through their phone.

Affects

The other team is protected by

Passcodes

If not protected, the other team loses two data tokens

Inside Threat

Attempted purchase

Attempted purchase

You try to buy something through the other team's devices.

Affects

The other team is protected by

BUY

Turn off automatic purchases

If not protected, the other team loses £30

Inside Threat

Deleted data

Deleted data

You try to delete all the data from the other team's devices.

Affects

The other team is protected by

Back up devices

If not protected, the other team loses two data tokens

Inside Threat

Inappropriate Content

Inappropriate content

You try to access content you should not through the other team's devices.

Affects

The other team is protected by

Family discussion about security

or

Profiles

If not protected, the other team loses two data tokens

Inside Threat

Altering device preferences

Altering device preferences

You try to alter the way the devices are set up to work automatically by the other team.

Affects

The other team is protected by

Passcodes

If not protected, the other team loses £40

Inside Threat

Annoyed neighbour

Annoyed neighbour

The next door neighbour is angry at the other team. You tell them to access and break the other team's devices, as the neighbour thinks they have the wifi password.

Affects

The other team is protected by

Change router password

If not protected, the other team loses two data tokens

Inside Threat

Nosy intruders

Nosy intruders

You're feeling nosy, and decide to set the other team's devices up to record them using cameras and microphones in their devices.

Affects

The other team is protected by

Tape over camera

or

Unplug devices

If not protected, the other team loses two data tokens

Inside Threat

Virus

Virus

You plug a USB stick with a virus on into the other team's laptop, to see if the virus will affect their devices.

Affects

The other team is protected by

Anti virus software

or

Guest network

If not protected, the other team loses £30

Inside Threat

Pet attack

Pet attack

You leave your pet in a room with the other team's device.

Affects

Roll the dice

Roll an even number: The pet wanders off. The device is unharmed: no action is needed.

Roll an odd number: The pet breaks the device. The other team must pay £50 for repairs.

Inside Threat

Stolen device

Stolen device

You decide to take the other team's devices.

Affects

The other team is protected by

Delete device history

If not protected, the other team loses two data tokens

Outside Threat

Hacking default passwords

Hacking default passwords

A hacker tries to use devices with default passwords to commit cyber crime.

You are protected if you have

Strong, Unique Passwords or Change router password or Password manager

If you are not protected, you lose two data tokens

Outside Threat

Accessing network through software weakness

Accessing network through software weakness

A hacker tries to access your information by using a weakness in your device software.

You are protected if you have

Guest network

If you are not protected, you lose two data tokens

Outside Threat

Forgotten account data breach

Forgotten account data breach

You forget to close an account. You find out that data linked to that account has been stolen.

You are protected if you have

Strong, Unique Passwords or Password manager

If you are not protected, you lose two data tokens

Outside Threat

Stolen smartphone

Stolen smartphone

Your smartphone has been stolen.

You are protected if you have

Passcodes

Even if you're protected, pay £50 towards a new smartphone

If you are not protected, you lose two data tokens

Outside Threat

Device software weakness

Device software weakness

The software on your device has a weakness. This can be exploited.

You are protected if you have

Automatic software updates

If you are not protected, roll the dice

Roll an even number: You are unaffected: no action is needed.

Roll an odd number: Your device is exploited. Lose two data tokens.

Outside Threat

Malicious device access

Malicious device access

A hacker accesses your devices with cameras, and intends to share access details on the dark web for anyone who wants it.

You are protected if you have

Tape over camera

If you are not protected, you lose two data tokens

Outside Threat

Malicious access to login details

Malicious access to login details

Someone gets holds of the login and password details for one of your devices.

You are protected if you have

Authenticator app

If you are not protected, you lose two data tokens

Outside Threat

Power surge destroying device

Power surge destroying device

There is a power surge, and your device is destroyed.

You are protected if you have

Back up devices

Even if you're protected, pay £50 towards a new device

If you are not protected, you lose two data tokens

Outside Threat

Device manufacturer goes out of business

Device manufacturer goes out of business

The company that has made one of your devices goes out of business.

You have to replace your device and lose access to all your data.

Pay £50 towards a new device

Lose two data tokens

Outside Threat

Burglary

Burglary

Your house is burgled, and your device is stolen.

You have to replace your device and lose access to all your data.

Pay £50 towards a new device

Lose two data tokens

Quiz

How does the UK's National Cyber Security Centre recommend you create strong, unique passwords?

A) Use a long string of letters and numbers and symbols and never write them down.

B) Choose three random words and use them as one long pass phrase.

C) Use a base password, and alter it slightly for each account.

D) Use a password manager.

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: B or D (either or both is fine!)

Quiz

How might you set up your home network to separate your home IoT devices from your smartphones and computers?

A) Using your router to create a guest network.

B) Get a second Internet connection in the house.

C) Connect smartphones and laptops to the Internet with mobile data only.

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: A

Quiz

Which of these might a cyber criminal be able to get from your device?

A) Physical Address
B) When you are on holiday or away from home
C) Voice recordings
D) Video recordings
E) Information about all family members
F) Passwords for other accounts
G) Contacts
H) Maybe all of the above

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: H

Quiz

How old do you have to be to have an account on most platforms and all social media sites in the UK?

A) 5

B) 10

C) 13

D) 16

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: C

Quiz

How might free apps make money from their users?

A) Collect and sell data about the user and their device.

B) Might encourage users to buy things within the service/app.

C) Might show adverts within the service/app.

D) Might limit free functionality unless the user pays (or give a free trial).

E) Maybe all of the above.

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: E

Quiz

How might a ransomware attack on your device's manufacturer affect your device?

A) Device may no longer be able to do anything on the Internet.

B) You might not be able to access any account information.

C) Your personal data may be stolen and given to others without your permission.

D) There may not be any effect.

E) All of the above are possible.

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: E

Quiz

Is performing a factory reset enough to delete all your data associated with a device?

A) Yes

B) No

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: B – factory reset will wipe data from the device, but will not delete any other data stored by the manufacturer linked to your account.

Quiz

Why do apps need updating on devices?

A) To fix weaknesses that have been found since the last update.

B) To add new features and functionality.

C) To slow down your device.

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: A and B – if both aren't mentioned, the question hasn't been fully answered!

Quiz

Which government organisation is responsible for giving UK citizens advice for protecting themselves when using technology?

A) Department for Education

B) National Cyber Security Centre

C) Cabinet Office

D) National Crime Agency

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: B

Quiz

For how long does a typical smartphone receive automatic software updates?

A) Android 2-3 years, Apple 5-6 years

B) Android 6-7 years, Apple 4-5 years

C) Android 1-2 years, Apple 2-3 years

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: A

Quiz

How are password managers designed to help with creating secure, unique passwords?

A) Because once you've decided the password to use you can type them in and look them up later.

B) Because they can automatically generate passwords and autofill when you need (so you don't have to remember each password).

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: B

Quiz

When you use a device, where does the data typically get processed and stored by the manufacturer?

A) On the device.

B) The data is not stored.

C) On the manufacturer's physical servers, or in the cloud (servers that are distributed globally and accessed through the Internet).

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: C

Quiz

What does an authenticator app do?

A) Provides two-factor authentication (another level of security) for accounts.

B) Acts as a password.

C) Stores your login details.

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: A

Quiz

How do you change a router password?

A) Contact your Internet Service Provider (ISP).

B) Log into the router using its IP address.

C) You can't.

Get the answer right? Choose a cyber security card from the pile.

Quiz

Answer: B

Cyber security card

Back up devices

Back up devices

Cost

★★★★★★½ 6.5 stars out of 10

Ease of set up

★★★ 3 stars out of 10

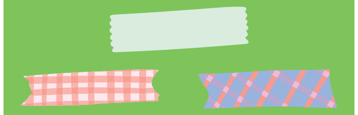
No further attention needed

★★ 2 stars out of 10

Whole family benefits

★★★½ 3.5 stars out of 10

Cyber security card



Tape over camera

Tape over camera

Cost

★★★★★★★★★½ 9.5 stars out of 10

Ease of set up

★★★★★★★★★½ 9.5 stars out of 10

No further attention needed

★★½ 2.5 stars out of 10

Whole family benefits

★★★★★★½ 6.5 stars out of 10

Cyber security card

Unplug devices

Unplug devices

Cost

★★★★★★★★★★ 10 stars out of 10

Ease of set up

★★★★★★★★★★ 10 stars out of 10

No further attention needed

★★ 2 stars out of 10

Whole family benefits

★★★★★★★★★★ 10 stars out of 10

Cyber security card

Family discussion about security

Family discussion about security

Cost

★★★★★★★★ 8 stars out of 10

Ease of set up

★★★★★★½ 6.5 stars out of 10

No further attention needed

★★★ 3 stars out of 10

Whole family benefits

★★★★★★★★½ 8.5 stars out of 10

Cyber security card

Password manager

Password manager

Cost

★★★★½ 4.5 stars out of 10

Ease of set up

★★ 2 stars out of 10

No further attention needed

★½ 1.5 stars out of 10

Whole family benefits

★★★ 3 stars out of 10

Cyber security card

Authenticator app

Authenticator app

Cost

★★★★★★★★½ 8.5 stars out of 10

Ease of set up

★★★★★½ 5.5 stars out of 10

No further attention needed

★★★½ 3.5 stars out of 10

Whole family benefits

★★½ 2.5 stars out of 10

Cyber security card

Turn off automatic purchases

Turn off automatic purchases

Cost

★★★★★★★★★ 9 stars out of 10

Ease of set up

★★★★★★★⯪ 7.5 stars out of 10

No further attention needed

★★★★★★★⯪ 7.5 stars out of 10

Whole family benefits

★★★★★★★★ 8 stars out of 10

Cyber security card

Anti-virus software

Anti-virus software

Cost

★★★★ 4 stars out of 10

Ease of set up

★★★⯪ 3.5 stars out of 10

No further attention needed

★★★★ 4 stars out of 10

Whole family benefits

★★★★ 4 stars out of 10

Cyber security card

Automatic software updates

Automatic software updates

Cost

★★★★★★★★★⯪ 9.5 stars out of 10

Ease of set up

★★★★★★★★⯪ 8.5 stars out of 10

No further attention needed

★★★★★★ 6 stars out of 10

Whole family benefits

★★★★★★★⯪ 7.5 stars out of 10

Cyber security card

Delete device history

Delete device history

Cost

★★★★★★★⯪ 7.5 stars out of 10

Ease of set up

★★★★★★ 6 stars out of 10

No further attention needed

★ 1 star out of 10

Whole family benefits

★★★★⯪ 4.5 stars out of 10

Cyber security card

Change router password

Change router password

Cost

★★★★★★★★★ 9 stars out of 10

Ease of set up

★⯪ 1.5 stars out of 10

No further attention needed

★★★★★ 5 stars out of 10

Whole family benefits

★★★★★★★★★⯪ 9.5 stars out of 10

Cyber security card

Guest Network

Guest Network

Cost

★★★★★★★ 7 stars out of 10

Ease of set up

★ 1 star out of 10

No further attention needed

★★★★★★⯪ 6.5 stars out of 10

Whole family benefits

★★★★★★★★★ 9 stars out of 10

Cyber security card

Profiles

Profiles

Cost

★★★★★★★★★ 9 stars out of 10

Ease of set up

★★★★★★⯪ 6.5 stars out of 10

No further attention needed

★★★★★★★ 7 stars out of 10

Whole family benefits

★★★★★★★ 7 stars out of 10

Cyber security card

Passcodes

Passcodes

Cost

★★★★★★★★★★ 10 stars out of 10

Ease of set up

★★★★★★★★ 8 stars out of 10

No further attention needed

★★★★★★★★⯪ 8.5 stars out of 10

Whole family benefits

★★★★★⯪ 5.5 stars out of 10

Cyber security card

Strong, Unique Passwords

Strong, Unique Passwords

Cost

★★★★★★★★ 8 stars out of 10

Ease of set up

★★★★★ 5 stars out of 10

No further attention needed

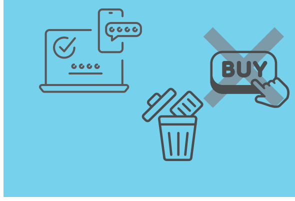
★★ 2 stars out of 10

Whole family benefits

★★★★★★★★ 8 stars out of 10

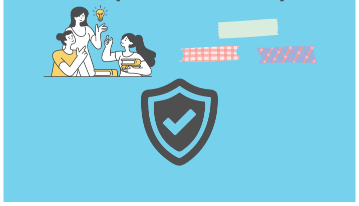
Device: Smart Speaker

Can be protected by these cyber security cards (as well as others!):



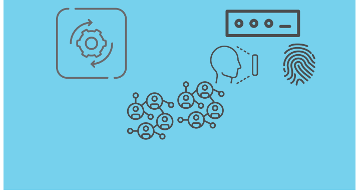
Device: Smart TV

Can be protected by these cyber security cards (as well as others!):



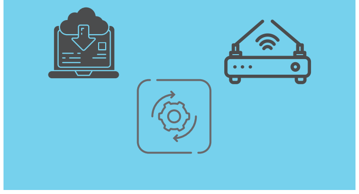
Device: Smart Thermostat

Can be protected by these cyber security cards (as well as others!):



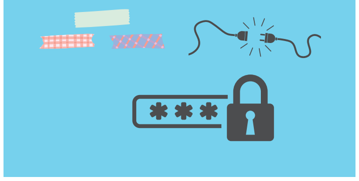
Device: Smart Vacuum

Can be protected by these cyber security cards (as well as others!):



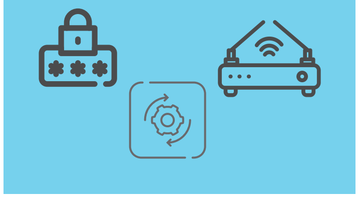
Device: Smart CCTV

Can be protected by these cyber security cards (as well as others!):



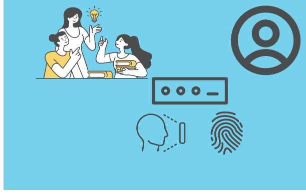
Device: Smart Bulb

Can be protected by these cyber security cards (as well as others!):



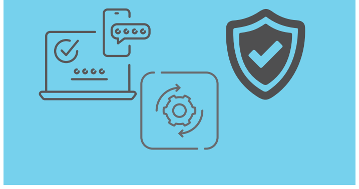
Device: Smart Lock

Can be protected by these cyber security cards (as well as others!):



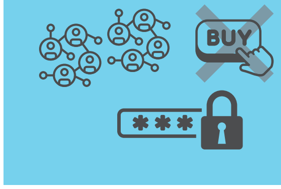
Device: Smart Plug

Can be protected by these cyber security cards (as well as others!):



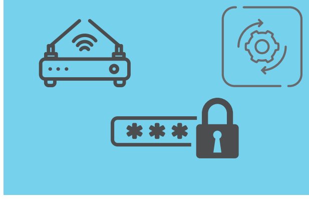
Device: Smart Fridge

Can be protected by these cyber security cards (as well as others!):



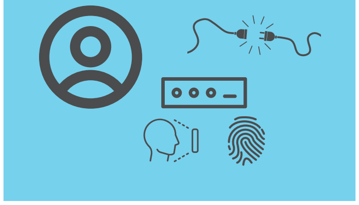
Device: Smart Washing Machine

Can be protected by these cyber security cards (as well as others!):



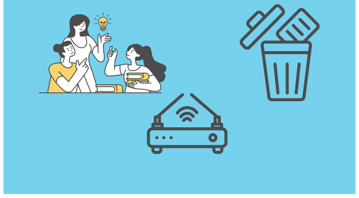
Device: Smart Coffee Machine

Can be protected by these cyber security cards (as well as others!):



Device: Smart Kettle

Can be protected by these cyber security cards (as well as others!):



Bibliography

Abaquita, D. et al. (2020). Privacy Norms within the Internet of Things Using Contextual Integrity. In *Companion Proceedings of the 2020 ACM International Conference on Supporting Group Work*, New York, NY, USA: Association for Computing Machinery, GROUP '20, p. 131–134.

Abdi, N., Ramokapane, K. M. and Such, J. M. (2019). More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA: USENIX Association, pp. 451–466.

Abrams, L. (2022). Apple security updates fix 2 zero-days used to hack iPhones, Macs. News report, Bleeping Computer, `https://www.bleepingcomputer.com/news/security/apple-security-updates-fix-2-zero-days-used-to-hack-iphones-macs/`.

Abras, C. et al. (2004). User-Centered Design. *Bainbridge, W Encyclopedia of Human-Computer Interaction Thousand Oaks: Sage Publications*, 37(4), pp. 445–456.

Abt, C. C. (1987). *Serious Games.* University Press of America.

Agha, Z. et al. (2021). 'Just-in-Time' Parenting: A Two-Month Examination of the Bi-directional Influences Between Parental Mediation and Adolescent Online Risk Exposure. In A. Moallem, ed., *HCI for Cybersecurity, Privacy and Trust*, Cham: Springer International Publishing, pp. 261–280.

Agrafiotis, I. et al. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1).

Ahmad, N. et al. (2018). Cyber security situational awareness among parents. In *Proceedings of the 2018 Cyber Resilience Conference (CRC)*, IEEE, pp. 21–23.

Albayram, Y., Liu, J. and Cangonj, S. (2021). Comparing the Effectiveness of Text-Based and Video-Based Delivery in Motivating Users to Adopt a Password Manager. In *Proceedings of the 2021 European Symposium on Usable Security*, New York, NY, USA: Association for Computing Machinery, EuroUSEC '21, p. 89–104.

Alsoubai, A. et al. (2022). From 'friends with benefits' to 'sextortion:' a nuanced investigation of adolescents' online sexual risk experiences. *Proc ACM Hum-Comput Interact*, 6(CSCW2).

Amadeo, R. (2022). Amazon alexa is a "colossal failure," on pace to lose $10 billion this year. `https://arstechnica.com/gadgets/2022/11/amazon-alexa-is-a-colossal-failure-on-pace-to-lose-10-billion-this-year/`.

Amankwa, E., Loock, M. and Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, pp. 248–252.

Anthi, E. et al. (2021). Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. *Computers & Security*, 108, p. 102352.

Apthorpe, N. et al. (2018). Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proc ACM Interact Mob Wearable Ubiquitous Technol*, 2(2).

Aufner, P. (2020). The IoT security gap: a look down into the valley between threat models and their implementation. *International Journal of Information Security*, 19, pp. 3–14.

Ayobi, A. et al. (2018). Flexible and Mindful Self-Tracking: Design Implications from Paper Bullet Journals. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '18, p. 1–14.

Bada, M., Sasse, A. and Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In *International Conference on Cyber Security for Sustainable Society*, Oxford, United Kingdom: Sustainable Society Network+, pp. 118–131.

Beneteau, E. et al. (2019). Communication Breakdowns Between Families and Alexa. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '19, p. 1–13.

Beneteau, E. et al. (2020). Parenting with Alexa: Exploring the Introduction of Smart Speakers on Family Dynamics. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '20, p. 1–13.

Bernd, J., Abu-Salma, R. and Frik, A. (2020). Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, USENIX Association.

Blackwell, L., Gardiner, E. and Schoenebeck, S. (2016). Managing Expectations: Technology Tensions among Parents and Teens. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, New York, NY, USA: Association for Computing Machinery, CSCW '16, p. 1390–1401.

Blandford, A., Furniss, D. and Makri, S. (2016). Paradigms and Strategies. In *Qualitative HCI Research: Going Behind the Scenes*, Cham: Springer International Publishing, chap. 6, pp. 61–78.

Blum-Ross, A. and Livingstone, S. (2020). *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives*. Oxford University Press.

Blythe, J. and Johnson, S. (2018). The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. In *Living in the Internet* *of Things: Cybersecurity of the IoT - 2018*, London, UK: Institution of Engineering and Technology, pp. 4–7.

Blythe, J. and Johnson, S. (2019). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 2019.

Blythe, J. M., Johnson, S. D. and Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, 9(1).

Boeckl, K. et al. (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. Tech. Rep. NIST Internal or Interagency Report (NISTIR) 8228, National Institute of Standards and Technology.

Boesen, J., Rode, J. A. and Mancini, C. (2010). The domestic panopticon: Location tracking in families. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, New York, NY, USA: ACM, pp. 65–74.

Boffi, L. (2020). Ding- Dong: The Storybell and Its Wizard. In *Proceedings of the Interaction Design and Children Conference*, New York, NY, USA: ACM, pp. 421–425.

Bogdan, R. and Taylor, S. J. (1975). *Introduction to Qualitative Research Methods: A Phenomenological Approach to the Social Sciences*. New York: Wiley.

Bolger, N., Davis, A. and Rafaeli, E. (2003). Diary methods: Capturing life as it is lived. *Annual Review of Psychology*, 54(1), pp. 579–616.

Bourdeau, S. et al. (2020). When Design Novices and LEGO® Meet: Stimulating Creative Thinking for Interface Design. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '20, p. 1–14.

Branley-Bell, D. et al. (2022). Exploring age and gender differences in ict cybersecurity behaviour. *Human Behavior and Emerging Technologies*, 2022.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), pp. 77–101.

Braun, V. and Clarke, V. (2021). *Thematic Analysis: A Practical Guide*. SAGE Publications.

Brignall, M. (2020). Bank fraud: couple lose £43,000 but can't get a refund. News report, The Guardian, `https://www.theguardian.com/money/2020/feb/08/bank-couple-lose-43000-but-cant-get-a-refund`.

Brosch, A. (2018). Sharenting - why do parents violate their children's privacy? *New Educational Review*, 54(4), pp. 75–85.

Brown, S. L., Manning, W. D. and Stykes, J. B. (2015). Family structure and child well-being: Integrating family complexity. *Journal of Marriage and Family*, 77(1), pp. 177–190.

Bryman, A. (2006). Integrating quantitative and qualitative research: how is it done? *Qualitative Research*, 6(1), pp. 97–113.

Buil-Gil, D. et al. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior*, p. 107770.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, pp. 523–548.

Byrne, S. et al. (2014). Peers, Predators, and Porn: Predicting Parental Underestimation of Children's Risky Online Experiences. *Journal of Computer-Mediated Communication*, 19(2), pp. 215–231.

Cannizzaro, S. et al. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. *PLOS ONE*, 15(5), p. e0231615.

Carter, S. and Mankoff, J. (2005). When participants do the capturing: The role of media in diary studies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, p. 899–908.

Çetin, O. et al. (2019). Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai. In *NDSS*, pp. 1–15.

Chalhoub, G. et al. (2020). Factoring user experience into the security and privacy design of smart home devices: A case study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI EA '20, p. 1–9.

Chalhoub, G. et al. (2021). "it did not give me an option to decline": A longitudinal analysis of the user experience of security and privacy in smart home products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, pp. 1–16.

Chandler, D. and Munday, R. (2011). Interpretivism. A Dictionary of Media and Communication (1 ed.), Oxford University Press.

Chang, H. (2016). *Autoethnography as Method*. New York, NY, USA: Routledge, 1st edn.

Chang, Z. (2019). Iot device security locking out risks and threats to smart homes. `https://documents.trendmicro.com/assets/white_papers/IoT-Device-Security.pdf`.

Chapple, M. et al. (2021). *CISSP Certified Information Systems Security Professional: Official Study Guide*. John Wiley & Sons.

Chatterjee, R. et al. (2018). The Spyware Used in Intimate Partner Violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA: 2018 IEEE Symposium on Security and Privacy (SP), pp. 441–458.

Cheng, Y. et al. (2018). Why Doesn't It Work? Voice-Driven Interfaces and Young Children's Communication Repair Strategies. In *Proceedings of the 17th ACM Conference on Interaction Design and Children*, New York, NY, USA: Association for Computing Machinery, IDC '18, p. 337–348.

Chhetri, C. (2019). Towards a Smart Home Usable Privacy Framework. In *Companion Publication of the 2019 Conference on Computer Supported Cooperative Work and Social Computing*, New York, NY, USA: Association for Computing Machinery, CSCW '19 Companion, p. 43–46.

Chhetri, C. and Genaro Motti, V. (2022). User-centric privacy controls for smart homes. *Proc ACM Hum-Comput Interact*, 6(CSCW2).

Childnet (2021). Have a conversation. `https://www.childnet.com/parents-and-carers/have-a-conversation/`.

Chothia, T. et al. (2017). Jail, Hero or Drug Lord? Turning a Cyber Security Course Into an 11 Week Choose Your Own Adventure Story. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, Vancouver, BC: USENIX Association, pp. 1–11.

Christensen, P. K., Skovgaard, C. O. and Petersen, M. G. (2019). Together Together: Combining Shared and Separate Activities in Designing Technology for Family Life. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, New York, NY, USA: ACM, pp. 374–385.

Christin, N. et al. (2012). It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice. In G. Danezis, ed., *Financial Cryptography and Data Security*, vol. 7035, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 16–30.

Clark, T. et al. (2021). *Bryman's Social Research Methods*. Oxford University Press.

Cobb, C. et al. (2020). How risky are real users' IFTTT applets? In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, USENIX Association, pp. 505–529.

Coleman, S. et al. (2017). The Internet on Our Own Terms: How Children and Young People Deliberated About Their Digital Rights. Tech. rep., 5Rights Foundation, `https://casma.wp.horizon.ac.uk/wp-content/uploads/2016/08/Internet-On-Our-Own-Terms.pdf`.

Coles-Kemp, L., Jensen, R. B. and Heath, C. P. R. (2020). Too much information: Questioning security in a post-digital society. In *Proceedings of the 2020 conference on human factors in computing systems*, New York, NY, USA: ACM, pp. 1–14.

Computer History Museum (2023). Timeline of Computer History. Tech. rep., `https://www.computerhistory.org/timeline/computers/`.

Coulton, P. and Lindley, J. G. (2019). More-Than Human Centred Design: Considering Other Things. *The Design Journal*, 22(4), pp. 463–481.

Cox, J. and Cole, S. (2019). How hackers are breaking into ring cameras. News report, Vice, `https://www.vice.com/en/article/3a88k5/how-hackers-are-breaking-into-ring-cameras`.

Cranor, L. F. et al. (2014). Parents' and Teens' Perspectives on Privacy in a Technology-Filled World. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, USA: USENIX Association, p. 19–35.

Creswell, J. (1994). *Research Design: Qualitative and Quantitative Approaches.* Sage Publications Thousand Oaks, CA.

Creswell, J. and Plano Clark, V. (2007). *Designing and conducting mexed methods research.* Thousand Oaks, CA: Sage Publications Thousand Oaks, CA.

Csikszentmihalyi, M. (1990). *Flow: The Psychology of Optimal Experience.* Harper & Row.

Cunningham, S. J. and Jones, M. (2005). Autoethnography: A tool for practice and education. In *Proceedings of the 6th ACM SIGCHI New Zealand Chapter's International Conference on Computer-Human Interaction: Making CHI Natural*, New York, NY, USA: Association for Computing Machinery, CHINZ '05, p. 1–8.

Czeskis, A. et al. (2010). Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, New York, NY, USA: Association for Computing Machinery, SOUPS '10.

Das, S., Dabbish, L. A. and Hong, J. I. (2019). A typology of perceived triggers for end-user security and privacy behaviors. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, Santa Clara, CA, USA: USENIX Association, pp. 97–115.

Data Protection and Digital Information Bill (2023). UK Government. https://bills.parliament.uk/bills/3322.

Datta Burton, S. et al. (2021). The UK Code of Practice for Consumer IoT Cybersecurity: where we are and what next. Tech. rep., Department for Digital, Culture, Media & Sport.

Davidson, J. et al. (2022). European Youth Cybercrime, Online Harm and Online Risk Taking: 2022 Research Report. Project report, United Kingdom Institute for Connected Communities, University of East London, https://repository.uel.ac.uk/item/8v59y.

Delamont, S. (2009). The only honest thing: autoethnography, reflexivity and small crises in fieldwork. *Ethnography and Education*, 4(1), pp. 51–63.

Denning, T., Shostack, A. and Kohno, T. (2014). Practical lessons from creating the Control-Alt-Hack card game and research challenges for games in education and research. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, San Diego, CA: USENIX Association, pp. 1–7.

Department for Digital, Culture, Media and Sport (2018). Code of practice for consumer IoT security. Governmental report, Department for Digital, Culture, Media and Sport, UK Government, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.

Department for Education (2013). National curriculum in England: computing programmes of study. Web page, https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study.

Department for Education (2022). Children looked after in england including adoptions. Web page, https://explore-education-statistics.service.gov.uk/find-statistics/children-looked-after-in-england-including-adoptions.

Department for Education, UK Government (2013). National curriculum in England: computing programmes of study. https://www.gov.uk/government/pu blications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study.

Digital Markets Act (2022). Digital Markets Act OJ L 265. http://data.europa.eu/eli/reg/2022/1925/oj.

Doctorow, C. (2019). *Unauthorized Bread*. Head of Zeus.

Dowthwaite, L. et al. (2020). "It's Your Private Information. It's Your Life.": Young People's Views of Personal Data Use by Online Technologies. In *Proceedings of the Interaction Design and Children Conference*, New York, NY, USA: Association for Computing Machinery, IDC '20, p. 121–134.

Druga, S. et al. (2017). "hey google is it ok if i eat you?": Initial explorations in child-agent interaction. In *Proceedings of the 2017 Conference on Interaction Design and Children*, New York, NY, USA: ACM, p. 595–600.

Druin, A. (2002). The role of children in the design of new technology. *Behaviour and information technology*, 21(1), pp. 1–25.

Dubois, D. J. et al. (2020). When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers. In *Proc. of the Privacy Enhancing Technologies Symposium (PETS)*, pp. 255–276.

Dupuis, M. et al. (2019). The Use and Non-Use of Cybersecurity Tools Among Consumers: Do They Want Help? In *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, ACM, p. 81–86.

Ehrenberg, N. and Keinonen, T. (2021). The technology is enemy for me at the moment: How smart home technologies assert control beyond intent. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, 401, pp. 1–11.

Ekambaranathan, A., Zhao, J. and Van Kleek, M. (2021). "Money Makes the World Go Around": Identifying Barriers to Better Privacy in Children's Apps From Developers' Perspectives. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '21, pp. 1–15.

Ellis, C., Adams, T. E. and Bochner, A. P. (2010). Autoethnography: An overview. *Forum Qualitative Sozialforschung*, 12(1).

Emami-Naeini, P. et al. (2019a). Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–12.

Emami-Naeini, P. et al. (2019b). Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '19, p. 1–12.

Emami-Naeini, P. et al. (2020). Ask the Experts: What Should Be on an IoT Privacy and Security Label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 447–464.

Eschler, J. (2016). A critical reflection on social media research using an autoethnographic approach. In *Proceedings of the 2016 49th Hawaii International Conference on System Sciences*, USA: IEEE Computer Society, HICSS '16, p. 1871–1880.

ETSI (2020). CYBER; cyber security for consumer Internet of Things: Baseline requirements. Tech. rep., ETSI, `https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf`.

European Commission (2022). Data Act: Commission proposes measures for a fair and innovative data economy. `https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113`.

European Commission (2023). Proposal for a Regulation amending Regulation (EU) 2019/881 as regards managed security services. `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208`.

Fabian, B., Ermakova, T. and Lentz, T. (2017). Large-scale readability analysis of privacy policies. In *Proceedings of the International Conference on Web Intelligence*, New York, NY, USA: Association for Computing Machinery, WI '17, p. 18–25.

Faklaris, C., Dabbish, L. and Hong, J. (2018). Adapting the transtheoretical model for the design of security interventions. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018).*

Fassl, M., Gröber, L. T. and Krombholz, K. (2021). Exploring user-centered security design for usable authentication ceremonies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '21.

Fernandes, E. et al. (2017). Security implications of permission models in smart-home application frameworks. *IEEE Security & Privacy*, 15(2), pp. 24–30.

Ferron, M. et al. (2019). A Walk on the Child Side: Investigating Parents' and Children's Experience and Perspective on Mobile Technology for Outdoor Child Independent Mobility. In *Proceedings of the 2019 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–12.

Financial Ombudsman (2021). Fraud and scams. Web page, `https://www.financial-ombudsman.org.uk/consumers/complaints-can-help/fraud-scams`.

Floros, G. et al. (2012). Influence of parental attitudes towards internet use on the employment of online safety measures at home. *Annual Review of CyberTherapy and Telemedicine*, 10, pp. 64–70.

Forbrukerradet (2016). #Toyfail: An analysis of consumer and privacy issues in three internet-connected toys. Tech. rep., Forbrukerradet, `https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf`.

Forget, A. et al. (2016). Do or Do Not, There is No Try: User Engagement May Not Improve Security Outcomes. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*, USA: USENIX Association, p. 97–111.

Fowler, B. (2018). Parents Should Be Cautious With Connected Toys, CR Testing Shows. *Consumer Reports*, `https://www.consumerreports.org/privacy/test-of-connected-toys-shows-parents-should-be-cautious`.

Frey, S. et al. (2019). The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering*, 45(5), pp. 521–536.

Furnell, S. (2022a). Assessing website password practices – unchanged after fifteen years? *Computers & Security*, 120, p. 102790.

Furnell, S. (2022b). Passwords: The cyber security lesson that was never learned? *Computer Fraud & Security*, 2022(8).

Furnell, S., Bryant, P. and Phippen, A. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, 26(5), pp. 410–417.

Furszyfer Del Rio, D., Sovacool, B. and Martiskainen, M. (2021). Controllable, frightening, or fun? exploring the gendered dynamics of smart home technology preferences in the united kingdom. *Energy Research & Social Science*, 77, p. 102105.

Gabriels, K. (2016). "I keep a close watch on this child of mine": a moral critique of other-tracking apps. *Ethics and Information Technology*, 18(3), pp. 175–184.

Gadlin, H. (1978). Child Discipline and the Pursuit of Self: An Historical Interpretation. In *Advances in Child Development and Behavior*, vol. 12, Elsevier, pp. 231–265.

Garcia, P. and Cifor, M. (2019). Expanding our reflexive toolbox: Collaborative possibilities for examining socio-technical systems using duoethnography. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW).

Garg, R. and Sengupta, S. (2019). "When You Can Do It, Why Can't I?": Racial and Socioeconomic Differences in Family Technology Use and Non-Use. *Proc ACM Hum-Comput Interact*, 3(CSCW).

Garitaonandia, C., Karrera, I. and Larranaga, N. (2019). Media convergence, risk and harm to children online. *Doxa Comunicacion*, 28, pp. 179–199.

Geeng, C. and Roesner, F. (2019). Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors* *in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI ’19, p. 1–13.

Ghosh, A. K. et al. (2018). Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI ’18, p. 1–14.

Gondree, M. and Peterson, Z. N. (2013). Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game. In *6th Workshop on Cyber Security Experimentation and Test (CSET 13)*, pp. 1–8.

Gondree, M., Peterson, Z. N. and Pusey, P. (2016). Talking about talking about cybersecurity games. *login Usenix Mag*, 41(1).

Goulden, M. (2019). “Delete the family”: platform families and the colonisation of the smart home. *Information, Communication & Society*, 0(0), pp. 1–18.

Griffioen, H. and Doerr, C. (2020). Examining mirai’s battle over the internet of things. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: Association for Computing Machinery, CCS ’20, p. 743–756.

Gulliksen, J. et al. (2003). Key principles for user-centred systems design. *Behaviour & Information Technology*, 22(6), pp. 397–409.

Gummer, T., Roßmann, J. and Silber, H. (2021). Using instructed response items as attention checks in web surveys: Properties and implementation. *Sociological Methods & Research*, 50(1), pp. 238–264.

Guo, J.-H. and Luh, W.-M. (2013). Efficient sample size allocation with cost constraints for heterogeneous-variance group comparison. *Journal of Applied Statistics*, 40(12), pp. 2549–2563.

Haggman, A. (2019). *Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education*. Ph.D. thesis, Royal Holloway, University of London.

Haney, J., Acar, Y. and Furman, S. (2021). "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In *Proceedings of the 30th USENIX Security Symposium*, USENIX Association, pp. 411–428.

Hariri, A., Giannelos, N. and Arief, B. (2020). Selective Forwarding Attack on IoT Home Security Kits. In S. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, C. Kalloniatis, J. Mylopoulos, A. Antón, S. Gritzalis, F. Pallas, J. Pohle, A. Sasse, W. Meng, S. Furnell and J. Garcia-Alfaro, eds., *Computer Security*, Cham: Springer International Publishing, pp. 360–373.

Harrabin, R. (2021). "Right to repair" law to come in this summer. News report, BBC News, `https://www.bbc.co.uk/news/business-56340077`.

Hart, S. et al. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95, p. 101827.

Hay Newman, L. (2022). Yes, it's time to ditch LastPass. *Wired*, `https://www.wired.com/story/lastpass-breach-vaults-password-managers/`.

Help Net Security (2022). Connected homes are expanding, so is attack volume. Help Net Security, `https://www.helpnetsecurity.com/2022/12/20/connected-homes-attack-volume/`.

Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New Security Paradigms workshop*, New York, NY, USA: ACM, pp. 133–144.

Hern, A. (2021). TechScape: How the UK forced global shift in child safety policies. News report, The Guardian, `https://www.theguardian.com/technology/2021/aug/18/uk-governments-child-safety-regulation-leads-to-global-policy-shifts`.

Hiniker, A., Schoenebeck, S. Y. and Kientz, J. A. (2016). Not at the Dinner Table: Parents- and Children-s Perspectives on Family Technology Rules. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, New York, NY, USA: ACM, pp. 1374–1387.

Hodges, D. (2021). Cyber-enabled burglary of smart homes. *Computers & Security*, 110, p. 102418.

Hodges-Schell, M. and O'Brien, J. (2015). Chapter 8 - living in the deliverables. In M. Hodges-Schell and J. O'Brien, eds., *Communicating the UX Vision*, Boston: Morgan Kaufmann, pp. 139–163.

Hong, M. K. et al. (2020). Using diaries to probe the illness experiences of adolescent patients and parental caregivers. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '20, p. 1–16.

Howe, A. E. et al. (2012). The Psychology of Security for the Home Computer User. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, USA: IEEE Computer Society, p. 209–223.

Howlett, M. (2022). Looking at the 'field' through a zoom lens: Methodological reflections on conducting online research during a global pandemic. *Qualitative Research*, 22(3), pp. 387–402.

Huang, Y., Obada-Obieh, B. and Beznosov, K. K. (2020). Amazon vs. My brother: How users of shared smart speakers perceive and cope with privacy risks. In *Proceedings of the 2020 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–13.

Hyers, L. L. (2018). *Diary Methods (Understanding Qualitiative Research).* Oxford, UK: Oxford University Press.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), pp. 83–95.

Ignatow, G. and Mihalcea, R. (2017). *Text Mining: A Guidebook for the Social Sciences.* Thousand Oaks, California: Sage Publications Thousand Oaks, CA.

Information Commissioner's Office (2020a). Age appropriate design: a code of practice for online services. `https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/`.

Information Commissioner's Office (2020b). Age Appropriate Design Code: 1. Best interests of the child . https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/.

Innocenzi, R. L. et al. (2018). Think Before You Click. Post. Type. *Journal of Cybersecurity Education, Research and Practice*, 1(3).

Iversen, O. S., Smith, R. C. and Dindler, C. (2017). Child as protagonist: Expanding the role of children in participatory design. In *Proceedings of the 2017 Conference on Interaction Design and Children*, New York, NY, USA: Association for Computing Machinery, IDC '17, p. 27–37.

Jaffray, A., Finn, C. and Nurse, J. R. (2021). Sherlocked: A detective-themed serious game for cyber security education. In *International Symposium on Human Aspects of Information Security and Assurance*, Springer, pp. 35–45.

Johnson, J. (2020). Market share held by the leading search engines in the United Kingdom (UK) as of June 2020. *Statista*, https://www.statista.com/statistics/280269/market-share-held-by-search-engines-in-the-united-kingdom/.

Jones, S. L. et al. (2019). What is 'cyber security'? differential language of cyber security across the lifespan. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI EA '19, p. 1–6.

Kilic, D. et al. (2022). The cardboard box study: understanding collaborative data management in the connected home. *Personal and Ubiquitous Computing*, 26(1), pp. 155–176.

Kim, I. and Kuljis, J. (2010). Applying content analysis to web-based content. *Journal of Computing and Information Technology*, 18(4), pp. 369–375.

Knowles, B. et al. (2019). A scenario-based methodology for exploring risks: Children and programmable iot. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, New York, NY, USA: ACM, p. 751–761.

Ko, M. et al. (2015). FamiLync: Facilitating participatory parental mediation of adolescents' smartphone use. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, New York, NY, USA: ACM, pp. 867–878.

Koumpouros, Y. and Toulias, T. (2020). User centered design and assessment of a wearable application for children with autistic spectrum disorder supporting daily activities. In *Proceedings of the 13th ACM International Conference on PErvasive Technologies Related to Assistive Environments*, New York, NY, USA: Association for Computing Machinery, PETRA '20.

Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal*, 29(2).

Kritzinger, E., Bada, M. and Nurse, J. R. C. (2017). A Study into the Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK. In M. Bishop, L. Futcher, N. Miloslavskaya and M. Theocharidou, eds., *Information Security Education for a Global Digital Society*, Cham: Springer International Publishing, pp. 110–120.

Kumar, P. et al. (2017). 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW), pp. 64:1–64:21.

Kung, F. Y., Kwok, N. and Brown, D. J. (2018). Are attention check questions a threat to scale validity? *Applied Psychology*, 67(2), pp. 264–283.

Lamond, M. et al. (2022). SOK: Young Children's Cybersecurity Knowledge, Skills & Practice: A Systematic Literature Review. In *Proceedings of the 2022 European Symposium on Usable Security*, New York, NY, USA: Association for Computing Machinery, EuroUSEC '22, p. 14–27.

Laughlin, A. (2020). Cheap smart plugs could expose you to hackers, or even cause a fire. *Which?*, `https://www.which.co.uk/news/2020/10/cheap-smart-plugs-could-expose-you-to-hackers-or-even-cause-a-fire`.

Laughlin, A. (2021). Smart Toys - Should You Buy Them? *Which?*, `https://www.which.co.uk/reviews/toys/article/smart-toys-should-you-buy-them`.

Laughlin, A. (2022). 5 things you need to know about smart devices. *Which?*, https://www.which.co.uk/news/article/5-things-you-need-to-know-about-smart-devices-a5IOE6h1rhxo.

Lee, K., Sjöberg, S. and Narayanan, A. (2022). Password policies of most top websites fail to follow best practices. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston, MA: USENIX Association, pp. 561–580.

Lee, M. et al. (2016). Security threat on wearable services: Empirical study using a commercial smartband. In *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, IEEE, pp. 1–5.

Lentzsch, C. et al. (2021). Hey Alexa, is this skill safe?: Taking a closer look at the Alexa skill ecosystem. In *Proceedings of the 28th ISOC Annual Network and Distributed Systems Symposium*, Internet Society, pp. 1–18.

Levelling Up, Housing and Communities Committee (2022). The Regulation of Social Housing. House of commons committee report, UK Parliament, https://publications.parliament.uk/pa/cm5803/cmselect/cmcomloc/18/report.html.

Li, J. et al. (2023). "It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit. *IEEE Symposium on Security and Privacy*, in press.

Liu, G. (2018). Funny accidental amazon Alexa ordering stories. https://www.digitaltrends.com/home/funny-accidental-amazon-alexa-ordering-stories/.

Living Wage Foundation (2022). What is the real living wage? Living Wage Foundation, https://www.livingwage.org.uk/what-real-living-wage.

Livingstone, S. and Sefton-Green, J. (2016). *The Class: Living and Learning in the Digital Age*. NYU Press.

Livingstone, S. et al. (2017). Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation: Maximizing Opportunities and Minimizing Risks. *Journal of Communication*, 67(1), pp. 82–105.

Loi, F. et al. (2017). Systematically Evaluating Security and Privacy for Consumer IoT Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, New York, NY, USA: ACM, pp. 1–6.

Lopez-Neira, I. et al. (2019). “Internet of Things”’: How abuse is getting smarter. *Safe Domestic Abuse Quarterly*, 63, pp. 22–26.

Lucero, A. (2018). Living without a mobile phone: An autoethnography. In *Proceedings of the 2018 Designing Interactive Systems Conference*, New York, NY, USA: Association for Computing Machinery, DIS ’18, p. 765–776.

Ludlow, D. (2022). How to fix the Philips Hue Lights unreachable error. `https://www.trustedreviews.com/how-to/fix-philips-hue-lights-unreachable-error-3631990`.

Lutz, C. and Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society*, 37(3), pp. 147–162.

Lyu, M. et al. (2017). Quantifying the reflective DDoS attack capability of household IoT devices. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 46–51.

Madani, R. et al. (2018). My smart remote: A smart home management solution for children. In *2018 1st International Conference on Computer Applications Information Security (ICCAIS)*, pp. 1–8.

Magee, L. (2011). Hermaneutics. In B. Cope, M. Kalantzis and L. Magee, eds., *Towards a Semantic Web*, Chandos Publishing, pp. 35–79.

Malinverni, L. and Pares, N. (2016). An autoethnographic approach to guide situated ethical decisions in participatory design with teenagers. *Interacting with Computers*, 29(3), pp. 403–415.

Manandhar, S. et al. (2020). Towards a Natural Perspective of Smart Homes for Practical Security and Safety Analyses. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy*, San Francisco, CA, USA: IEEE, pp. 482–499.

Manches, A. et al. (2015). Three Questions about the Internet of Things and Children. *TechTrends*, 59(1), pp. 76–83.

Mancini, C. et al. (2011). In the Best Families: Tracking and Relationships. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, p. 2419–2428.

Marczewski, A. (2018). *Gamification: Even Ninja Monkeys Like to Play: Unicorn Edition*. Independently Published.

Markwick, K. et al. (2019). Technology and Family Violence in the Context of Post-Separated Parenting. *Australian and New Zealand Journal of Family Therapy*, 40(1), pp. 143–162.

Mazurek, M. L. et al. (2010). Access control for home data sharing: evaluating social acceptability. In *Proceedings of the 28th international conference on Human factors in computing systems*, New York, NY, USA: ACM, p. 645.

McDonald, N., Schoenebeck, S. and Forte, A. (2019). Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW).

McHugh, B. C. et al. (2017). Most teens bounce back: Using diary methods to examine how quickly teens recover from episodic online risk exposure. *Proc ACM Hum-Comput Interact*, 1(CSCW).

McReynolds, E. et al. (2017). Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '17, p. 5197–5207.

Metatla, O. et al. (2019). Voice user interfaces in schools: Co-designing for inclusion with visually-impaired and sighted pupils. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '19, p. 1–15.

Michael, D. R. and Chen, S. L. (2005). *Serious Games: Games That Educate, Train, and Inform*. Muska & Lipman Premier-Trade.

Micom Lab (2022). Voice assistants & voice computing – cyber security and avoiding risk - micom labs. https://micomlabs.com/2022/01/20/voice-assistants-and-cyber-security-3/.

Mikulak, M. et al. (2022). 'Internet is easy if you know how to use it': Doing online research with people with learning disabilities during the COVID-19 pandemic. *British Journal of Learning Disabilities*.

Mills, A. M. and Sahi, N. (2019). An Empirical Study of Home User Intentions towards Computer Security. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Canterbury, New Zealand: Hawaii International Conference on System Sciences, pp. 4834–4840.

Minkus, T., Liu, K. and Ross, K. W. (2015). Children Seen But Not Heard: When Parents Compromise Children's Online Privacy. In *Proceedings of the 24th International Conference on World Wide Web*, New York, NY, USA: ACM, pp. 776–786.

Mitchell, V. et al. (2016). Empirical investigation of the impact of using co-design methods when generating proposals for sustainable travel solutions. *CoDesign*, 12(4), pp. 205–220.

Mohajeri Moghaddam, H. et al. (2019). Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: Association for Computing Machinery, CCS '19, p. 131–147.

Morris, R. and Thompson, K. (1979). Password security: A case history. *Commun ACM*, 22(11), p. 594–597.

Morrison, B., Coventry, L. and Briggs, P. (2021). How do older adults feel about engaging with cyber-security? *Human Behavior and Emerging Technologies*, 3(5), pp. 1033–1049.

Motherboard (2018). The Motherboard Guide to Not Getting Hacked. *Vice*, https://www.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide.

Mozilla Foundation (2021). Why we made this guide. https://foundation.mozilla.org/en/privacynotincluded/about/why/.

Muir, K. and Joinson, A. (2020). An exploratory study into the negotiation of cyber-security within the family home. *Frontiers in Psychology*, 11.

National Cyber Security Centre, UK (2019). Smart devices: using them safely in your home. https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home.

National Institute of Standards and Technology (n.d.a). NIST Computer Security Resource Center: Glossary - Risk. Tech. rep., https://csrc.nist.gov/glossary/term/risk.

National Institute of Standards and Technology (n.d.b). NIST Computer Security Resource Center: Glossary - Threat. Tech. rep., https://csrc.nist.gov/glossary/term/threat.

National Society for the Prevention of Cruelty to Children (NSPCC) (2020). Research with children: ethics, safety and avoiding harm. Web page, https://learning.nspcc.org.uk/research-resources/briefings/research-with-children-ethics-safety-avoiding-harm.

National Society for the Prevention of Cruelty to Children (NSPCC) (2022). Looked after children. Web page, https://learning.nspcc.org.uk/children-and-families-at-risk/looked-after-children.

Neuman, W. (1997). *Social Research Methods: Qualitative and Quantitative Approaches*. Allyn and Bacon.

Ng, A. (2022). Amazon gave ring videos to police without owners' permission. https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission-00045513.

Nicholson, J. et al. (2018). Simple nudges for better password creation. In *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32*, pp. 1–12.

Nicholson, J. et al. (2021a). Training and embedding cybersecurity guardians in older communities. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '21.

Nicholson, J. et al. (2021b). Understanding Young People's Experiences of Cybersecurity. In *European Symposium on Usable Security 2021*, pp. 200–210.

Nikken, P. and de Haan, J. (2015). Guiding young children's internet use at home: Problems that parents experience in their parental mediation and the need for parenting support. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 9(1), p. 1.

Nissenbaum, H. F. (2010). *Privacy in Context: technology, policy, and the integrity of social life*. Stanford, California: Stanford Law Books, an imprint of Standford University Press.

Nokia (2023). Nokia threat intelligence report finds malicious iot botnet activity has sharply increased. `https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/`.

Noor, P. (2019). Ring hackers are reportedly watching and talking to strangers via in-home cameras. News report, The Guardian, `https://www.theguardian.com/technology/2019/dec/13/ring-hackers-reportedly-watching-talking-strangers-in-home-cameras`.

Norman, D. (1986). User centered system design. *New perspectives on human-computer interaction*.

Noroozian, A. et al. (2021). Can ISPs help mitigate IoT malware? A longitudinal study of broadband ISP security efforts. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, pp. 337–352.

Nthala, N. (2019). *Home data security decisions*. PhD Thesis, University of Oxford.

Nthala, N. and Flechais, I. (2018). Informal support networks: an investigation into home data security practices. In *Fourteenth symposium on usable privacy and security*, Baltimore, MD: USENIX Association, pp. 63–82.

Nuhla, A. et al. (2018). Exploring parents' experience in guiding their children while using gadget at home. In *Proceedings of the 4th International Conference on Early Childhood Education (SECRET 2018)*, Semarang, Indonesia: Atlantis Press, pp. 22–46.

Nurse, J. R. C., Atamli, A. and Martin, A. (2016). Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home. In T. Tryfonas, ed., *Human Aspects of Information Security, Privacy, and Trust*, Cham: Springer International Publishing, pp. 255–267.

Oatley, K. and Djikic, M. (2008). Writing as thinking. *Review of General Psychology*, 12(1), pp. 9–27.

OConnor, T., Jessee, D. and Campos, D. (2021). Through the spyglass: Towards iot companion app man-in-the-middle attacks. In *Proceedings of the 14th Cyber Security Experimentation and Test Workshop*, New York, NY, USA: Association for Computing Machinery, CSET '21, p. 58–62.

Office for National Statistics (2021a). Families and households statistics explained. Web page, `https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/families/articles/familiesandhouseholdsstatisticsexplained/2021-03-02`.

Office for National Statistics (2021b). Population estimates for the uk, england and wales, scotland and northern ireland: mid-2020. Web page, `https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/bulletins/annualmidyearpopulationestimates/latest`.

Office for National Statistics (2022a). Employment and labour market. Web page, `https://www.ons.gov.uk/employmentandlabourmarket`.

Office for National Statistics (2022b). Families and households in the UK: 2021. Web page, `https://www.ons.gov.uk/peoplepopulationandcommunity/birt` hsdeathsandmarriages/families/bulletins/familiesandhouseholds/2021.

O'Kane, A. A., Rogers, Y. and Blandford, A. E. (2014). Gaining empathy for non-routine mobile device use through autoethnography. In *Proceedings of the 2014 SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '14, p. 987–990.

Oldfield, M. (2016). Unequal sample sizes and the use of larger control groups pertaining to power of a study.

Ouherrou, N. et al. (2023). Participatory design of an Arabic serious game for children with dyslexia: a qualitative exploratory study. *Universal Access in the Information Society*, pp. 1–23.

Oygür, I., Epstein, D. A. and Chen, Y. (2020). Raising the responsible child: Collaborative work in the use of activity trackers for children. *Proc ACM Hum-Comput Interact*, 4(CSCW2).

Pancratz, N. and Diethelm, I. (2020). "Draw Us How Smartphones, Video Gaming Consoles, and Robotic Vacuum Cleaners Look like from the inside": Students' Conceptions of Computing System Architecture. In *Proceedings of the 15th Workshop on Primary and Secondary Computing Education*, New York, NY, USA: Association for Computing Machinery, WiPSCE '20.

Park, S. and Lim, Y.-k. (2020). Investigating user expectations on the roles of family-shared AI speakers. In *Proceedings of the 2020 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–13.

Parkin, S. et al. (2019). Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change. *Proceedings of the Workshop on Usable Security and Privacy (USEC '19).*

Parkin, S. et al. (2020). Usability analysis of shared device ecosystem security: Informing support for survivors of iot-facilitated tech-abuse. In *Proceedings of the New Security Paradigms Workshop*, New York, NY, USA: Association for Computing Machinery, NSPW '19, p. 1–15.

Pattnaik, N., Li, S. and Nurse, J. R. (2023). A survey of user perspectives on security and privacy in a home networking environment. *ACM Comput Surv*, 55(9).

Paul, K. (2019). Ring sued by man who claims camera was hacked and used to harass his kids. https://www.theguardian.com/technology/2019/dec/27/ring-camera-lawsuit-hackers-alabama.

Paul, K. (2020). Dozens sue Amazon's ring after camera hack leads to threats and racial slurs. News report, The Guardian, https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats.

PayPal (Europe) S.à r.l. et Cie, S.C.A. (2021). Send money, pay online or set up a merchant account - PayPal. Web page, https://www.paypal.com/uk/home.

Pearson, K. (1900). X. on the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 50(302), pp. 157–175.

Pencheva, D., Hallett, J. and Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, 18(2), pp. 68–74.

Pfeffer, K. et al. (2022). Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston, MA: USENIX Association, pp. 1–18.

Pocock, T., Smith, M. and Wiles, J. (2021). Recommendations for virtual qualitative health research during a pandemic. *Qualitative Health Research*, 31(13), pp. 2403–2413.

Poole, E. S. et al. (2009). Computer help at home: methods and motivations for informal technical support. In *Proceedings of the Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 739–748.

Pothong, K. and Livingstone, S. (2022a). Chapter 11 – Consulting children during COVID-19: managing research ethics on Zoom. In S. Kotilainen, ed., *Methods* *in Practice: Studying children and youth online*, Hamburg: Leibniz-Institut für Medienforschung — Hans-Bredow-Institut (HBI), p. 59.

Pothong, K. and Livingstone, S. (2022b). Consulting children about their rights in a digital world to guide innovators and designers. `https://digitalfuturescommission.org.uk/blog/consulting-children-about-their-rights-in-a-digital-world-to-guide-innovators-and-designs/`.

Prange, S., von Zezschwitz, E. and Alt, F. (2019). Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, Stockholm, Sweden: IEEE European Symposium on Security and Privacy Workshops, pp. 154–158.

Prasad, A., Ruiz, R. and Stablein, T. (2019). Understanding Parents' Concerns with Smart Device Usage in the Home. In A. Moallem, ed., *HCI for Cybersecurity, Privacy and Trust*, vol. 11594, Cham: Springer International Publishing, pp. 176–190.

Prensky, M. (2007). *Digital Game-Based Learning*. Paragon House.

Prior, S. and Renaud, K. (2023). Who is best placed to support cyber responsibilized uk parents? *Children*, 10(7), `https://www.mdpi.com/2227-9067/10/7/1130`.

Product Security and Telecommunications Infrastructure Act (2022). UK Government. `https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted`.

Putnam, C. and Mobasher, B. (2020). Children with autism and technology use: A case study of the diary method. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI EA '20, p. 1–8.

Quayyum, F., Cruzes, D. S. and Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, p. 100343.

Quayyum, F. et al. (2021). Understanding Parents' Perceptions of Children's Cybersecurity Awareness in Norway. In *Proceedings of the Conference on Information Technology for Social Good*, New York, NY, USA: Association for Computing Machinery, GoodIT '21, p. 236–241.

Ramsetty, A. and Adams, C. (2020). Impact of the digital divide in the age of COVID-19. *Journal of the American Medical Informatics Association*, 27(7), pp. 1147–1148.

Ranger, S. (2020). The Internet of Things: The basics explained. *ZDNet*, `https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/`.

Rapp, A. (2018). Autoethnography in Human-Computer Interaction: Theory and Practice. In *New Directions in Third Wave Human-Computer Interaction*, Springer International Publishing, pp. 25–42.

Ray, L. (2019). We surveyed 1,400 searchers about Google - here's what we learned. Blog article, `https://moz.com/blog/new-google-survey-results`.

Redmiles, E. et al. (2020). A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *29th USENIX Security Symposium (USENIX Security 20)*, USENIX Association, pp. 89–108.

Renaud, K. and Shepherd, L. A. (2018). How to make privacy policies both GDPR-compliant and usable. In *Proceedings of 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment*, pp. 1–8.

Renaud, K. et al. (2018). Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security*, 78, pp. 198–211.

Riley, A. (2022). How your smart home devices can be turned against you. `https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse`.

Rode, J. A. (2010). The roles that make the domestic work. In *Proceedings of the 2010 ACM conference on Computer supported cooperative work*, New York, NY, USA: ACM, pp. 381–390.

Rode, J. A. (2011). A theoretical agenda for feminist HCI. *Interacting with Computers*, 23(5), pp. 393–400.

Rostami, A. et al. (2022). Being Hacked: Understanding Victims' Experiences of IoT Hacking. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston, MA: USENIX Association, pp. 613–631.

Schell, J. (2019). *The Art of Game Design, 3rd Edition.* A K Peters/CRC Press.

Seymour, W. et al. (2020). Informing the design of privacy-empowering tools for the connected home. In *Proceedings of the 2020 conference on human factors in computing systems*, New York, NY, USA: ACM, pp. 1–14.

Shams, J., Arachchilage, N. and Such, J. (2020). Vision: Why Johnny Can't Configure Smart Home? A Behavioural Framework for Smart Home Privacy Configuration. In *IEEE European Symposium on Security and Privacy*, IEEE, pp. 184–189.

Shank, D. B. et al. (2023). Discontinuance and restricted acceptance to reduce worry after unwanted incidents with smart home technology. *International Journal of Human–Computer Interaction*, 39(14), pp. 2771–2784.

Sheble, L. and Wildemuth, B. (2009). Research diaries. *Applications of social research methods to questions in information and library science*, pp. 211–221.

Shin, W. (2015). Parental socialization of children's Internet use: A qualitative approach. *New Media & Society*, 17(5), pp. 649–665.

Simonet, J. and Teufel, S. (2019). The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users. In G. Dhillon, F. Karlsson, K. Hedström and A. Zúquete, eds., *ICT Systems Security and Privacy Protection*, vol. 562, Cham: Springer International Publishing, pp. 194–208.

Singh, D. et al. (2018). Users' Perceptions and Attitudes Towards Smart Home Technologies. In M. Mokhtari, B. Abdulrazak and H. Aloulou, eds., *Smart Homes and Health Telematics, Designing a Better Future: Urban Assisted Living*, Cham: Springer International Publishing, pp. 203–214.

Slupska, J. and Tanczer, L. M. (2021). Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the Internet of Things. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Emerald Publishing Limited, pp. 663–688.

Smahel, D. et al. (2020). EU Kids Online 2020: Survey results from 19 countries. Tech. rep., EU Kids Online, `http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf`.

Soni, J. (2020). Avast reportedly sold user web browsing data. News report, Tech Radar, `https://www.techradar.com/news/avast-reportedly-sold-user-web-browsing-data`.

Sorbring, E. and Lundin, L. (2012). Mothers' and fathers' insights into teenagers' use of the Internet. *New Media & Society*, 14(7), pp. 1181–1197.

Sparapani, V. C. et al. (2023). Prototyping Process and Usability Testing of a Serious Game for Brazilian Children With Type 1 Diabetes. *CIN: Computers, Informatics, Nursing*, pp. 10–1097.

Staton, B. (2022). Why is personal finance not being taught more in schools? *Financial Times*, `https://www.ft.com/content/a385c715-3541-4eb7-8f41-19b9c21a41a1`.

Statt, N. (2018). Amazon sent 1,700 Alexa voice recordings to the wrong user following data request. *The Verge*, `https://www.theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings-wrong-user-gdpr-privacy-ai`.

Steinberg, S. (2017). Sharenting: Children's Privacy in the Age of Social Media. *Emory Law Journal*, 66, pp. 839–884.

Stevens, F. et al. (2021). The Applicability of the UK Computer Misuse Act 1990 onto Cases of Technology-Facilitated Domestic Violence and Abuse. *London: UK Home Office/University College London Publication forthcoming.*

Strengers, Y. et al. (2019). Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early

Adopters. In *Proceedings of the 2019 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–13.

Student Beans (2021). 89% of students think schools don't give sufficient financial education. *FE News*, `https://www.fenews.co.uk/skills/89-of-students-think-schools-dont-give-sufficient-financial-education/`.

Superti Pantoja, L. et al. (2020). Play-Based Design: Giving 3- to 4-Year-Old Children a Voice in the Design Process. In *Proceedings of the 2020 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–14.

Svenaeus, F. (2012). Hermeneutics. In R. Chadwick, ed., *Encyclopedia of Applied Ethics (Second Edition)*, San Diego: Academic Press, second edition edn., pp. 574–581.

Tabassum, M., Kosinski, T. and Lipford, H. R. (2019). "i don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA: USENIX Association, pp. 435–450.

Tabassum, M. et al. (2020). Smart home beyond the home: A case for community-based access control. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '20, p. 1–12.

Tanczer, L. M. et al. (2018). Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK: Institution of Engineering and Technology, pp. 1–9.

Taneski, V., Heričko, M. and Brumen, B. (2019). Systematic overview of password security problems. *Acta Polytechnica Hungarica*, 16(3), pp. 143–165.

Tang, J., Birrell, E. and Lerner, A. (2022). Replication: How well do my results generalize now? the external validity of online privacy and security surveys. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston, MA: USENIX Association, pp. 367–385.

Tang, X. et al. (2022). “I Never Imagined Grandma Could Do So Well with Technology”: Evolving Roles of Younger Family Members in Older Adults’ Technology Learning and Use. *Proc ACM Hum-Comput Interact*, 6(CSCW2).

techUK and GfK (2021). The state of the connected home 2021. Industry report, techUK, https://www.techuk.org/resource/the-state-of-the-connected-home-2021-new-report-launch.html.

techUK and GfK (2022). The state of the connected home 2022. Industry report, techUK, https://www.techuk.org/resource/state-of-the-connected-home-2022.html.

Thakkar, P. K. et al. (2022). “It Would Probably Turn into a Social Faux-Pas”: Users’ and Bystanders’ Preferences of Privacy Awareness Mechanisms in Smart Homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI ’22, pp. 1–13.

Thompson, N., McGill, T. J. and Wang, X. (2017). “Security begins at home”: Determinants of home computer and mobile device security behavior. *Computers & Security*, 70, pp. 376–391.

Tolmie, P. et al. (2016). “This has to be the cats”: Personal Data Legibility in Networked Sensing Systems. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, New York, NY, USA: ACM, pp. 491–502.

Toulas, B. (2023). TP-link smart bulbs can let hackers steal your WIFI password. https://www.bleepingcomputer.com/news/security/tp-link-smart-bulbs-can-let-hackers-steal-your-wifi-password/.

Trend Micro (2017). Securing Your Routers Against Mirai and Other Home Network Attacks. https://www.trendmicro.com/vinfo/pl/security/news/internet-of-things/securing-routers-against-mirai-home-network-attacks.

Trotman, A. (2021). Let’s face it, we have to stop using passwords. https://ne ws.microsoft.com/en-gb/features/lets-face-it-we-have-to-stop-using-passwords/.

Turner, S., Pothong, K. and Livingstone, S. (2022). Education Data Reality: The challenges for schools in managing children's education data. Tech. rep., Digital Futures Commission. 5 Rights Foundation, London, UK, https://digitalfuturescommission.org.uk/wp-content/uploads/2022/06/Education-data-reality-report.pdf.

Turner, S. et al. (2021). The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society*, 23(10), pp. 2861–2881.

Ur, B., Jung, J. and Schechter, S. (2014). Intruders versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, New York, NY, USA: ACM, p. 129–139.

Vailshery, L. (2022). Number of IoT connected devices worldwide 2019-2021, with forecasts to 2030. *Statista*, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide.

Vasalou, A., Oostveen, A.-M. and Joinson, A. N. (2012). A case study of non-adoption: the values of location tracking in the family. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, New York, NY, USA: ACM, pp. 779–788.

Vass, L. (2020). Android pulls 24 'dangerous' malware-filled apps from Play Store. News report, Naked Security, https://nakedsecurity.sophos.com/2020/02/06/android-pulls-24-dangerous-malware-filled-apps-from-play-store/.

Verweij, D. (2019). Exploring future IoT for families through end user development: Applying do-it-together practises to reveal family dynamics in technology adoption. In *Extended Abstracts of the 2019 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–4.

Vetrivel, S. et al. (2023). Examining Consumer Reviews to Understand Security and Privacy Issues in the Market of Smart Home Devices. *32nd USENIX Security Symposium*, in press.

Wang, J. et al. (2017). Quantified baby: Parenting and the use of a baby wearable in the wild. *Proc ACM Hum-Comput Interact*, 1(CSCW).

Wash, R. (2010). Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, Redmond, Washington: ACM, pp. 1–16.

Wash, R. et al. (2014). Out of the loop: How automated software updates cause unintended security consequences. In *10th symposium on usable privacy and security*, Menlo Park, CA: USENIX Association, pp. 89–104.

Watson, H. et al. (2020). "We hold each other accountable": Unpacking how social groups approach cybersecurity and privacy together. In *Proceedings of the 2020 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–12.

Waugh, R. (2023). How "smart" home devices like doorbells and thermostats are allowing hackers to commit "digital burglaries" - and what you can do to shore-up your security. `https://www.dailymail.co.uk/sciencetech/article-11718501/Danger-smart-home-devices-like-doorbells-thermostats.html`.

White, M. D. and Marsh, E. E. (2006). Content analysis: A flexible methodology. *Library trends*, 55(1), pp. 22–45.

Williams, K. et al. (2019). Understanding Family Collaboration Around Lightweight Modification of Everyday Objects in the Home. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW).

Williams, M., Nurse, J. R. and Creese, S. (2019). (Smart)Watch Out! encouraging privacy-protective behavior through interactive games. *International Journal of Human-Computer Studies*, 132, pp. 121–137.

Williams, M., Nurse, J. R. C. and Creese, S. (2016). The Perfect Storm: The Privacy Paradox and the Internet-of-Things. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Salzberg: International Conference on Availability, Reliability and Security, pp. 644–652.

Williams, M., Nurse, J. R. C. and Creese, S. (2017). Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, Calgary: Conference on Privacy, Security and Trust, pp. 181–189.

Winder, D. (2020). Use a smart lock? get in the sea, 73% of security professionals say. `https://www.forbes.com/sites/daveywinder/2020/08/16/use-a-smart-lock-get-in-the-sea-73-of-security-professionals-say/`.

Windl, M. and Mayer, S. (2022). The skewed privacy concerns of bystanders in smart environments. *Proc ACM Hum-Comput Interact*, 6(MHCI).

Wisniewski, P. et al. (2016). Dear diary: Teens reflect on their weekly online risk experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '16, p. 3919–3930.

Wisniewski, P. et al. (2017a). Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, New York, NY, USA: ACM, pp. 51–69.

Wisniewski, P. et al. (2017b). Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, New York, NY, USA: ACM, pp. 523–540.

Xu, Y. and Warschauer, M. (2020). What are you talking to?: Understanding children's perceptions of conversational agents. In *Proceedings of the 2020 Conference on Human Factors in Computing Systems*, Honolulu, HI, USA: ACM, pp. 1–13.

Yan, C. et al. (2022). A survey on voice assistant security: Attacks and countermeasures. *ACM Comput Surv*, 55(4).

Yao, Y. et al. (2019a). Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, CHI '19, p. 1–12.

Yao, Y. et al. (2019b). Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), pp. 59:1–59:24.

Yap, C. E. L. and Lee, J.-J. (2020). "Phone Apps Know a Lot about You!": Educating Early Adolescents about Informational Privacy through a Phygital Interactive Book. In *Proceedings of the Interaction Design and Children Conference*, New York, NY, USA: ACM, pp. 49–62.

Yardi, S. and Bruckman, A. (2011). Social and technical challenges in parenting teens' social media use. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, p. 3237.

Yip, J. C. et al. (2019). Laughing is Scary, but Farting is Cute: A Conceptual Model of Children's Perspectives of Creepy Technologies. In *Proceedings of the 2019 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–15.

Ylizaliturri-Salcedo, M. A. et al. (2018). Building security bubbles: Design of a wearable device for child tracking in vulnerable zones. In *Proceedings of the 7th Mexican Conference on Human-Computer Interaction*, New York, NY, USA: Association for Computing Machinery, MexIHC '18.

Zahir, S. et al. (2015). Protection and deception: Discovering game theory and cyber literacy through a novel board game experience. *arXiv preprint arXiv:150505570*.

Zeng, E., Mare, S. and Roesner, F. (2017). End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security*, Santa Clara, CA: USENIX Association, pp. 65–80.

Zhao, J. et al. (2019). “I make up a silly name”: Understanding Children’s Perception of Privacy Risks Online. In *Proceedings of the 2019 Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1–13.

Zheng, S. et al. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), pp. 200:1–200:20.

Zimmermann, V. et al. (2019). Vision: Shining light on smart homes – supporting informed decision-making of end users. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, Stockholm, Sweden: IEEE, pp. 149–153.

Zou, Y. et al. (2019). You ‘might’ be affected: An empirical analysis of readability and usability issues in data breach notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, p. 1–14.